(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 582 086 A1**

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
17.04.2013 Bulletin 2013/16

(21) Application number: **11809745.0**

(22) Date of filing: **22.07.2011**

(51) Int Cl.:
H04L 9/08 *(2006.01)*

(86) International application number:
PCT/JP2011/066716

(87) International publication number:
WO 2012/011575 (26.01.2012 Gazette 2012/04)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **23.07.2010 JP 2010166401**

(71) Applicant: **Nippon Telegraph And Telephone Corporation**
Tokyo 100-8116 (JP)

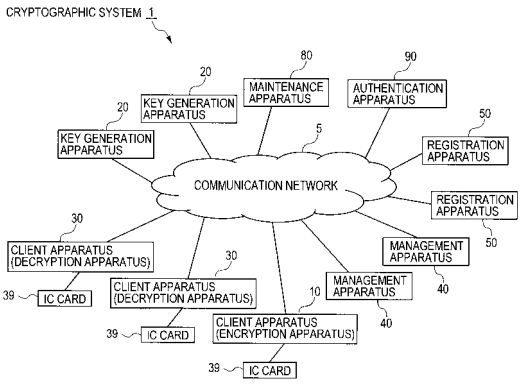
(72) Inventors:
- **KOBAYASHI, Tetsutaro**
  Musashino-shi
  Tokyo 180-8585 (JP)
- **TAKEUCHI, Kaku**
  Musashino-shi
  Tokyo 180-8585 (JP)
- **CHIKARA, Sakae**
  Musashino-shi
  Tokyo 180-8585 (JP)

(74) Representative: **MERH-IP**
Matias Erny Reichl Hoffmann
Paul-Heyse-Strasse 29
80336 München (DE)

(54) CRYPTOSYSTEM, CRYPTOGRAPHIC COMMUNICATION METHOD, ENCRYPTION DEVICE, KEY-GENERATING DEVICE, DECRYPTION DEVICE, CONTENT SERVER DEVICE, PROGRAM, AND RECORDING MEDIUM

(57) A cryptographic communication technology that is based on functional encryption and that can operate flexibly is provided. A conversion rule information pair is determined in advance, which has attribute conversion rule information prescribing a conversion rule for converting attribute designation information to attribute information used in a functional encryption algorithm and logical expression conversion rule information prescribing a conversion rule for converting logical expression designation information to logic information used in the functional encryption algorithm. One kind of conversion rule information included in the conversion rule information pair is used to obtain first attribute information or first logic information from input information. The first attribute information or the first logic information is used for encryption. Encryption information is decrypted with a decryption key generated by using second attribute information or second logic information obtained from user information by using the other kind of conversion rule information.

FIG.1



EP 2 582 086 A1

Description

[TECHNICAL FIELD]

[0001] The present invention relates to a cryptographic communication technology, and more specifically, to a cryptographic communication technology based on functional encryption.

[BACKGROUND ART]

[0002] Known cryptographic technologies include a common key cryptosystem and a public key cryptosystem.

[0003] In the common key cryptosystem, a message sender encrypts a message with a common key to obtain an encrypted message, and the receiver decrypts the encrypted message with the same common key to obtain the original message. Therefore, it is necessary to establish a procedure for the sender and receiver to possess the common key securely.

[0004] In the public key cryptosystem, (1) a receiver prepares a public key and a private key corresponding thereto, (2)a sender encrypts a message with the public key to obtain an encrypted message, and (3) the receiver decrypts the encrypted message with the private key to obtain the original message. Therefore, the sender needs to obtain the public key prepared by the receiver before encrypting the message. In other words, encryption is impossible unless the receiver generates the public key.

[0005] Predicate encryption has been proposed recently. In the predicate encryption, information X is embedded in an encrypted message during encryption by the sender, the receiver who has information Y having a specific relationship with the information X can decrypt the encrypted message or obtain information related to the message without knowing the message. The sender does not necessarily need to know the information Y possessed by the receiver during encryption. In addition, the sender does not necessarily need to determine the receiver before encryption. The sender can determine the information X actively, freely and with initiative. In theory, the information X is called an attribute I (variable) and the information Y is called a predicate f (propositional function or Boolean function). The specific relationship which the information X and the information Y need to satisfy during decryption is, for example, f(I) = true.

[PRIOR ART LITERATURE]

[NON-PATENT LITERATURE]

[0006]

Non-patent literature 1: Information Security Project of NTT Information Sharing Platform Laboratories, "NTT Cryptographic Primitives", URL: http://info.isl.ntt.co.jp/crypt/camellia/technology.html, retrieved on July 15, 2010

Non-patent literature 2: J. Katz, A. Sahai, and B. Waters, "Predicate Encryption Supporting Disjunction, Polynomial Equations, and Inner Products", Eurocrypt 2008, pp. 146-162

[SUMMARY OF THE INVENTION]

[PROBLEMS TO BE SOLVED BY THE INVENTION]

[0007] An object of the present invention is to provide a cryptographic communication technology that is based on functional encryption and that can operate flexibly.

[MEANS TO SOLVE THE PROBLEMS]

[0008] A first aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression des-

ignation information) to logical information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

Each of the one or the plurality of decryption apparatuses uses the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm.

[0009] Alternatively, the first aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;

Each of the one or the plurality of decryption apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and uses a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

[0010] Alternatively, the first aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the

plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

Each of the one or the plurality of decryption apparatuses uses the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm.

[0011] Alternatively, the first aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm.

Each of the one or the plurality of decryption apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and uses a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a key generation process of using the second

attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

[0012] A second aspect of the present invention will be outlined below.

In a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and a plurality of decryption apparatuses, a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses; one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

Each of the one or the plurality of decryption apparatuses uses the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm. The decryption apparatus also performs a transfer process of transferring the encryption information to another decryption apparatus. The encryption information to be transferred may be sent from the encryption apparatus or may be transferred from another decryption apparatus. At least a part of the decryption apparatuses included in the cryptographic system has a function of performing the transfer process, but all of the decryption apparatuses are not required to have this function. A decryption apparatus that has received the transferred encryption information asks the key generation apparatus to generate the decryption key, if necessary, and performs the decryption process.

[0013] Alternatively, the second aspect of the present invention will be outlined below.

In a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and a plurality of decryption apparatuses, a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses; one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an

encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;

Each of the one or the plurality of decryption apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and uses a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

The decryption apparatus also performs a transfer process of transferring the encryption information to another decryption apparatus. The encryption information to be transferred may be sent from the encryption apparatus or may be transferred from another decryption apparatus. At least a part of the decryption apparatuses included in the cryptographic system has a function of performing the transfer process, but all of the decryption apparatuses are not required to have this function. A decryption apparatus that has received the transferred encryption information asks the key generation apparatus to generate the decryption key, if necessary, and performs the decryption process.

[0014] Alternatively, the second aspect of the present invention will be outlined below.

In a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and a plurality of decryption apparatuses, a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses; one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

Each of the one or the plurality of decryption apparatuses uses the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm. The decryption apparatus also performs a transfer process of transferring the encryption information to another decryption apparatus. The encryption information to be transferred may be sent from the encryption apparatus or may be transferred from another decryption apparatus. At least a part of the decryption apparatuses included in the cryptographic system has a function of performing the transfer process, but all of the decryption apparatuses are not required to have this function. A decryption apparatus that has received the transferred encryption information asks the key generation apparatus to generate the decryption key, if necessary, and performs the decryption process.

[0015] Alternatively, the second aspect of the present invention will be outlined below.

In a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and a plurality of decryption apparatuses, a private key and

a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses; one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm.

Each of the one or the plurality of decryption apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and uses a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm.

Each of the one or the plurality of key generation apparatuses performs a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

The decryption apparatus also performs a transfer process of transferring the encryption information to another decryption apparatus. The encryption information to be transferred may be sent from the encryption apparatus or may be transferred from another decryption apparatus. At least a part of the decryption apparatuses included in the cryptographic system has a function of performing the transfer process, but all of the decryption apparatuses are not required to have this function. A decryption apparatus that has received the transferred encryption information asks the key generation apparatus to generate the decryption key, if necessary, and performs the decryption process.

[0016] A third aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, one or a plurality of decryption apparatuses, and one or a plurality of content servers.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting

the content with the common key, according to the functional encryption algorithm.

Each of the one or the plurality of content servers stores the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and transmits the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus.

Each of the one or the plurality of key generation apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

Each of the one or the plurality of decryption apparatuses performs a process of an acquisition request of the encrypted content for the content server; uses the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm; performs a content acquisition process of decrypting the encrypted content obtained from the content server with the common key obtained in the decryption process; and displays content obtained by decrypting the encrypted content.

[0017] Alternatively, the third aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, one or a plurality of decryption apparatuses, and one or a plurality of content servers.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm.

Each of the one or the plurality of content servers stores the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and transmits the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus.

Each of the one or the plurality of decryption apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; uses a decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm; performs a content acquisition process of decrypting the encrypted content obtained from the content server, with the common key obtained in the decryption process; and displays content obtained by decrypting the encrypted content.

Each of the one or the plurality of key generation apparatuses performs a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

[0018] Alternatively, the third aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, one or a plurality of decryption apparatuses, and one or a plurality of content servers.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm.

Each of the one or the plurality of content servers stores the encrypted content sent from each of the one or the plurality of encryption apparatuses; and transmits the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus.

Each of the one or the plurality of key generation apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encrypted content.

Each of the one or the plurality of decryption apparatuses performs a process of an acquisition request of the encrypted content for the content server; uses the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm; and displays content obtained by decrypting the encrypted content.

[0019] Alternatively, the third aspect of the present invention will be outlined below.

A cryptographic system that uses functional encryption includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, one or a plurality of decryption apparatuses, and one or a plurality of content servers.

A private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses.

One or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm.

Policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance.

Each of the one or the plurality of encryption apparatuses performs a first propositional logic information acquisition process of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and an

encryption process of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm.

Each of the one or the plurality of content servers stores the encrypted content sent from each of the one or the plurality of encryption apparatuses; and transmits the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus.

Each of the one or the plurality of decryption apparatuses performs a second propositional logic information acquisition process of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; uses a decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm; and displays content obtained by decrypting the encrypted content.

Each of the one or the plurality of key generation apparatuses performs a key generation process of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encrypted content.

[EFFECTS OF THE INVENTION]

[0020] According to the present invention, by using one piece of conversion rule information selected based on whether input information input to an encryption apparatus is attribute designation information or logical expression designation information, where the one piece of conversion rule information is either one of attribute conversion rule information and logical expression conversion rule information contained in one conversion rule information pair selected from conversion rule information pairs, the attribute information or the logic information is obtained from the input information; therefore, cryptographic communication based on functional encryption can be operated in a flexible manner.

[BRIEF DESCRIPTION OF THE DRAWINGS]

[0021]

Fig. 1 is a structural view of a cryptographic system according to each embodiment in a first aspect of the present invention;

Fig. 2 is a view (No. 1) showing a processing procedure of a cryptographic communication method according to each embodiment in the first aspect;

Fig. 3 is a view (No. 2) showing the processing procedure of the cryptographic communication method according to each embodiment in the first aspect;

Fig. 4 is a view (No. 3) showing the processing procedure of the cryptographic communication method according to each embodiment in the first aspect;

Fig. 5 is a functional block diagram of an encryption apparatus according to a first embodiment of the first aspect;

Fig. 6 is a view showing a detailed processing procedure of an encryption process according to the first embodiment of the first aspect;

Fig. 7 is a functional block diagram of a decryption apparatus according to the first embodiment of the first aspect;

Fig. 8 is a view showing a detailed processing procedure of a decryption process according to the first embodiment of the first aspect;

Fig. 9 is a functional block diagram of a key generation apparatus according to the first embodiment of the first aspect;

Fig. 10 is a view showing a detailed processing procedure of a key generation process according to the first embodiment of the first aspect;

Fig. 11 is a view showing how to obtain attribute information or predicate information from input information or user information by using a schema corresponding to a policy;

Fig. 12 is a view showing how to obtain attribute information from attribute designation information by using an attribute schema;

Fig. 13 is a view showing how to obtain predicate information from predicate designation information by using a predicate schema;

Fig. 14 is a view showing examples of policies;

Fig. 15 is a view showing an example decryption key table;

Fig. 16 is a view showing an example authentication table;

Fig. 17 is a view showing an example user information tables;

Fig. 18 is a functional block diagram of a decryption apparatus according to a second embodiment of the first aspect;

Fig. 19 is a view showing a detailed processing procedure of a decryption process according to the second embodiment of the first aspect;
Fig. 20 is a functional block diagram of a key generation apparatus according to the second embodiment of the first aspect;
Fig. 21 is a view showing a detailed processing procedure of a key generation process according to the second embodiment of the first aspect;
Fig. 22 is a functional block diagram of an encryption apparatus according to a third embodiment of the first aspect;
Fig. 23 is a view showing a detailed processing procedure of an encryption process according to the third embodiment of the first aspect;
Fig. 24 is a functional block diagram of a decryption apparatus according to the third embodiment of the first aspect;
Fig. 25 is a view showing a detailed processing procedure of a decryption process according to the third embodiment of the first aspect;
Fig. 26 is a functional block diagram of a decryption apparatus according to a fourth embodiment of the first aspect;
Fig. 27 is a view showing a detailed processing procedure of a decryption process according to the fourth embodiment of the first aspect;
Fig. 28 is a structural view of a cryptographic system according to each embodiment in a second aspect of the present invention;
Fig. 29 is a view (No. 1) showing a processing procedure of a cryptographic communication method according to each embodiment in the second aspect;
Fig. 30 is a view (No. 2) showing the processing procedure of the cryptographic communication method according to each embodiment in the second aspect;
Fig. 31 is a view (No. 3) showing the processing procedure of the cryptographic communication method according to each embodiment in the second aspect;
Fig. 32 is a view (No. 4) showing the processing procedure of the cryptographic communication method according to each embodiment in the second aspect;
Fig. 33 is a functional block diagram of an encryption apparatus according to a first embodiment of the second aspect;
Fig. 34 is a view showing a detailed processing procedure of an encryption process according to the first embodiment of the second aspect;
Fig. 35 is a functional block diagram of a first decryption apparatus according to the first embodiment of the second aspect;
Fig. 36 is a view showing a detailed processing procedure of a first decryption process according to the first embodiment of the second aspect;
Fig. 37 is a functional block diagram of a second decryption apparatus according to the first embodiment of the second aspect;
Fig. 38 is a view showing a detailed processing procedure of a second decryption process according to the first embodiment of the second aspect;
Fig. 39 is a functional block diagram of a key generation apparatus according to the first embodiment of the second aspect;
Fig. 40 is a view showing a detailed processing procedure (corresponding to the first decryption apparatus) of a key generation process according to the first embodiment of the second aspect;
Fig. 41 is a view showing a detailed processing procedure (corresponding to the second decryption apparatus) of a key generation process according to the first embodiment of the second aspect;
Fig. 42 is a functional block diagram of a first decryption apparatus according to a second embodiment of the second aspect;
Fig. 43 is a view showing a detailed processing procedure of a first decryption process according to the second embodiment of the second aspect;
Fig. 44 is a functional block diagram of a second decryption apparatus according to the second embodiment of the second aspect;
Fig. 45 is a view showing a detailed processing procedure of a second decryption process according to the second embodiment of the second aspect;
Fig. 46 is a functional block diagram of a key generation apparatus according to the second embodiment of the second aspect;
Fig. 47 is a view showing a detailed processing procedure (corresponding to the first decryption apparatus) of a key generation process according to the second embodiment of the second aspect;
Fig. 48 is a view showing a detailed processing procedure (corresponding to the second decryption apparatus) of a key generation process according to the second embodiment of the second aspect;
Fig. 49 is a functional block diagram of an encryption apparatus according to a third embodiment of the second aspect;
Fig. 50 is a view showing a detailed processing procedure of an encryption process according to the third embodiment

of the second aspect;
Fig. 51 is a functional block diagram of a first decryption apparatus according to the third embodiment of the second aspect;
Fig. 52 is a view showing a detailed processing procedure of a first decryption process according to the third embodiment of the second aspect;
Fig. 53 is a functional block diagram of a second decryption apparatus according to the third embodiment of the second aspect;
Fig. 54 is a view showing a detailed processing procedure of a second decryption process according to the third embodiment of the second aspect;
Fig. 55 is a functional block diagram of a first decryption apparatus according to a fourth embodiment of the second aspect;
Fig. 56 is a view showing a detailed processing procedure of a first decryption process according to the fourth embodiment of the second aspect;
Fig. 57 is a functional block diagram of a second decryption apparatus according to the fourth embodiment of the second aspect;
Fig. 58 is a view showing a detailed processing procedure of a second decryption process according to the fourth embodiment of the second aspect;
Fig. 59 is a view showing an example structure of data exchanged when the present invention is applied to an email system or an instant messaging system;
Fig. 60 is a structural view of a cryptographic system according to each embodiment in a third aspect of the present invention;
Fig. 61 is a view (No. 1) showing a processing procedure of a cryptographic communication method according to each embodiment in the third aspect;
Fig. 62 is a view (No. 2) showing the processing procedure of the cryptographic communication method according to each embodiment in the third aspect;
Fig. 63 is a view (No. 3) showing the processing procedure of the cryptographic communication method according to each embodiment in the third aspect;
Fig. 64 is a view (No. 4) showing the processing procedure of the cryptographic communication method according to each embodiment in the third aspect;
Fig. 65 is a functional block diagram of an encryption apparatus according to a first embodiment of the third aspect;
Fig. 66 is a view showing a detailed processing procedure of an encryption process according to the first embodiment of the third aspect;
Fig. 67 is a functional block diagram of a content server according to the first embodiment of the third aspect;
Fig. 68 is a functional block diagram of a decryption apparatus according to the first embodiment of the third aspect;
Fig. 69 is a view showing a detailed processing procedure of a second decryption process according to the first embodiment of the third aspect;
Fig. 70 is a functional block diagram of a key generation apparatus according to the first embodiment of the third aspect;
Fig. 71 is a view showing a detailed processing procedure of a key generation process according to the first embodiment of the third aspect;
Fig. 72 is a functional block diagram of a decryption apparatus according to a second embodiment of the third aspect;
Fig. 73 is a view showing a detailed processing procedure of a decryption process according to the second embodiment of the third aspect;
Fig. 74 is a functional block diagram of a key generation apparatus according to the second embodiment of the third aspect;
Fig. 75 is a view showing a detailed processing procedure of a key generation process according to the second embodiment of the third aspect;
Fig. 76 is a functional block diagram of an encryption apparatus according to a third embodiment of the third aspect;
Fig. 77 is a view showing a detailed processing procedure of an encryption process according to the third embodiment of the third aspect;
Fig. 78 is a functional block diagram of a decryption apparatus according to the third embodiment of the third aspect;
Fig. 79 is a view showing a detailed processing procedure of a decryption process according to the third embodiment of the third aspect;
Fig. 80 is a functional block diagram of a decryption apparatus according to a fourth embodiment of the third aspect;
Fig. 81 is a view showing a detailed processing procedure of a decryption process according to the fourth embodiment of the third aspect;
Fig. 82 is a view showing an example structure of data exchanged when the present invention is applied to a content delivery system;

Fig. 83 is a view illustrating tree structure data that expresses a standard logical expression PRO(1)∧PRO(2)∨¬PRO(3) including: propositional variables PRO(1) and PRO(2); a negation ¬PRO(3) of a propositional variable PRO(3); and logical symbols ∨ and v; and

Fig. 84 is a view illustrating tree structure data that expresses a standard logical expression PRO(1)∧PRO(2)∨PRO(2)∧PRO(3)∨PRO(1)∧PRO(3)∨¬PRO(4)∨(¬PRO(5) ∧PRO(6))∧PRO(7) including: propositional variables PRO(1), PRO(2), PRO(3), PRO(6), and PRO(7); negations ¬PRO(4) and zero(5) of propositional variables PRO(4) and PRO(5); and logical symbols ∧ and v.

[DETAILED DESCRIPTION OF THE EMBODIMENTS]

<Outline of Functional Encryption>

[0022] In recent years, extended encryption of ID-based encryption called functional encryption is attracting attention. The functional encryption is formed of the following four algorithms (Setup, KeyGen, Enc, Dec). The protocol thereof will be outlined below.

«Protocol FE»

[0023] ==========

· Setup $(1^{\lambda}) \rightarrow$ (pk, sk): setup algorithm

[0024] A probability polynomial time algorithm that receives a security parameter 1^{λ} and outputs a public parameter pk and a master key sk

· KeyGen (sk, i) $\rightarrow sk_i$: key generation algorithm

[0025] A probability polynomial time algorithm that receives the master key sk and a key identifier i and outputs a private key sk_i corresponding to the key identifier i

· Enc (pk, j, x) $\rightarrow c_j$: encryption algorithm

[0026] A probability polynomial time algorithm that receives the public parameter pk, a receiver identifier j, and information to be encrypted (plaintext) x and outputs a ciphertext c_j

· Dec (pk, sk_i, c_j) $\rightarrow$ y: decryption algorithm

[0027] A probability polynomial time algorithm that receives the public parameter pk, the private key sk_i, and the ciphertext c_j and outputs a plaintext y

[0028] ==========

[0029] In the functional encryption, the validity of the ID-based encryption is extended, and a receiver of a ciphertext can evaluate some function $f_{i,j}(x)$ concerning the plaintext x on the basis of the private key having the key identifier i and the ciphertext having the receiver identifier j. That is, if a given function $f_{j,j}(x)$ exists and if a probability Pr represented by Expression (A) to ∀i, ∀j, $\forall x \in \{0, 1\}^{poly(\lambda)}$ is overwhelming to λ (a difference from 1 is negligible), the functional encryption (Setup, KeyGen, Enc, Dec) is regarded as valid. Note that poly(λ) represents the polynomial length determined by λ.

$$\Pr\left[y = f_{i,j}(x) \middle| \begin{array}{l} (pk, sk) \leftarrow Setup(1^{\lambda}) \\ sk_i \leftarrow KeyGen(sk, i) \\ c_j \leftarrow Enc(pk, j, x) \\ y \leftarrow Dec(pk, sk_i, c_j) \end{array} \right] \quad \cdots (A)$$

[0030] In particular, a given relationship R(·, ·) exists, and functional encryption having a function $f_{j,j}(x)$ of type repre-

sented by Expression (B) contains various types of encryption (⊥ is a symbol that represents that normal decryption cannot be made).

$$f_{i,j}(x) = \begin{cases} x & (R(i,j) : True) \\ \perp & (R(i,j) : False) \end{cases} \quad \cdots (B)$$

[0031] For example, the ID-based encryption can be defined as functional encryption having a function $f_{j\cdot j}(x)$ represented by Expression (C).

$$f_{i,j}(x) = \begin{cases} x & (i = j) \\ \perp & (i \neq j) \end{cases} \quad \cdots (C)$$

[0032] Various types of functional encryption having a more advanced relationship R(·, ·) have been studied. The most versatile one of these types of functional encryption, which is called attribute-based encryption (ABE), predicate encryption (PE), or the like, has been actively studied. In 2010, Tatsuaki Okamoto et al. proposed this type of functional encryption that is relatively practical, corresponds to a predicate of a polynomial size and a set of predicate variables, and can prove CCA safety against adaptive identifier attacks under standard cryptologic assumptions (see reference literature R1). (reference literature R1) Tatsuaki Okamoto and Katsuyuki Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption", In: Advances in Cryptology -- CRYPTO 2010, Lecture Notes in Computer Science, Volume 6223, 191-208, Springer-Verlag, 2010, Full paper: http://eprint.iacr.org/2010/563/

[0033] Functional encryption having a relationship R(·, ·) that is represented by Expression (D) assuming that the key identifier i and the receiver identifier j are instances of a predicate and a predicate variable, respectively, is called key policy functional encryption. At this time, the case where the ciphertext conceals not only the plaintext x but also the instance j of the predicate variable is called attribute concealment.

$$R(i,j) = \begin{cases} True & (\text{The receiver identifier j satisfies the predicate i.}) \\ False & (\text{The receiver identifier j does not satisfy the predicate i.}) \end{cases} \quad \cdots (D)$$

[0034] Functional encryption having a relationship R(·, ·) that is represented by Expression (E) assuming that the key identifier i and the receiver identifier j are instances of a predicate variable and a predicate, respectively, is called ciphertext policy functional encryption. At this time, the case where the ciphertext conceals not only the plaintext x but also the predicate j is called predicate concealment.

$$R(i,j) = \begin{cases} True & (\text{The key identifier i satisfies the predicate j.}) \\ False & (\text{The key identifier i does not satisfy the predicate j.}) \end{cases} \quad \cdots (E)$$

[0035] Key policy functional encryption having attribute concealment or ciphertext policy functional encryption having predicate concealment is called predicate encryption (see reference literature R2). (reference literature R2) Tatsuaki Okamoto and Katsuyuki Takashima, "Hierarchical Predicate Encryption for Inner-Products", ASIACRYPT 2009: pp. 214-231, 2009.

<Threshold Gate>

[0036] The configuration of a threshold gate in the functional encryption is achieved according to a threshold secret sharing scheme, that is, a t-out-of-N secret sharing scheme, in which a secret can be restored if arbitrary t pieces out of N pieces of sharing information are given, whereas the secret cannot be restored even if arbitrary (t - 1) or less pieces of sharing information are given. For the t-out-of-N secret sharing, please see reference literature R3 and the like. The threshold gate according to the t-out-of-N secret sharing scheme is called a t-out-of-N threshold gate. The t-out-of-N

threshold gate has a gate structure that outputs "true" if t or more conditions out of N conditional expressions of inputs are satisfied, and outputs "false" in the other cases. The negation (of an output) of the t-out-of-N threshold gate is equivalent to an (N - t + 1)-out-of-N threshold gate of the negation (of every input). (reference literature R3) A. Shamir, "How to Share a Secret", Communications of the ACM, November 1979, Volume 22, Number 11, pp. 612-613.

<Private Key Verifiable Functional Encryption>

[0037] Functional encryption that can definitely prove that the private key sk_i is created correctly for the key identifier i is called private key verifiable functional encryption. A non-interactive zero-knowledge proof (see reference literature R4) that proves that key generation procedures have been performed correctly is added to the private key, whereby the private key verifiable functional encryption can be configured. The use of the private key verifiable functional encryption proves definitely that the private key sk_i is created correctly for the key identifier i. (reference literature R4) Jens Groth and Amit Sahai, "Efficient Non-interactive Proof Systems for Bilinear Groups", Advances in Cryptology - EUROCRYPT 2008, LNCS 4965, pp. 415-432, March 2010.

<Ciphertext Publicly Verifiable Functional Encryption>

[0038] Functional encryption that can definitely prove that a ciphertext is created correctly even without any key for the ciphertext, the key being obtained according to the KeyGen algorithm, is called ciphertext publicly verifiable functional encryption. A non-interactive zero-knowledge proof (see reference literature R4 given above) that proves that encryption procedures have been performed correctly is added to the ciphertext, whereby the ciphertext publicly verifiable functional encryption can be configured. The use of the ciphertext publicly verifiable functional encryption proves definitely that the same results can be obtained even if any key capable of decryption is used for the ciphertext.

<Electronic Signature>

[0039] The electronic signature refers to the following three algorithms ($KeyGen_\Sigma$, $Sign_\Sigma$, $Verify_\Sigma$). The protocol thereof will be outlined below.

[0040] <<Protocol ES>>

[0041] ==========

$KeyGen_\Sigma\ (1^\lambda) \rightarrow (sk_\Sigma, pk_\Sigma)$: key generation algorithm

[0042] A probability polynomial time algorithm that receives a security parameter 1^λ and outputs a public key for electronic signature verification pk_Σ and a private key for electronic signature sk_Σ

· $Sign_\Sigma\ (sk_\Sigma, m) \rightarrow \sigma$: signature algorithm

[0043] A probability polynomial time algorithm that receives the private key for electronic signature sk_Σ and signature target information m and outputs a signature σ

· $Verify_\Sigma\ (pk_\Sigma, m, \sigma) \rightarrow 0 / 1$: signature verification algorithm

[0044] A probability polynomial time algorithm that receives the public key for electronic signature verification pk_Σ, the signature target information m, and the signature σ and outputs a verification result (Rejection (0) or Acceptance (1))
==========

[0045] Note that there is proposed an electronic signature scheme that can prove existential unforgeability against adaptive selected document attacks under appropriate cryptologic assumptions (for example, RSA-PSS (see reference literature R5)).
(reference literature R5) Atsushi Fujioka, Evaluation Report on Cryptographic Algorithm RSA-PSS, Nippon Telegraph and Telephone Corporation, 2001

[0046] Next, the outline of the functional encryption will be described. Symbols and the like will be defined prior to the description.

[Definitions]

[0047] Matrix: A rectangular arrangement of elements of a set in which a calculation is defined. Not only elements of a ring but also elements of a group can form a matrix.

$(\cdot)^T$: Transposed matrix of ·
$(\cdot)^{-1}$: Inverse matrix of ·
$\wedge$: Logical symbol representing a logical AND
v: Logical symbol representing a logical OR
¬: Logical symbol representing a negation (NOT)
Propositional variable: Variable in a set {true, false} having "true" or "false" of a statement as its element. The propositional variable and the negation of the propositional variable are collectively referred to as a literal.
Logical expression: Expression having formal grammar representing a statement in mathematical logic. Specifically, "true" and "false" are logical expressions, a propositional variable is a logical expression, the negation of a logical expression is a logical expression, the logical AND of a logical expression and a logical expression is a logical expression, and the logical OR of a logical expression and a logical expression is a logical expression.
Z: Set of integers
sec: Security parameter (sec $\in$ Z, sec > 0)
0*: Sequence formed of * zeros
1*: Sequence formed of * ones

[0048] F_q: Finite field of order q, where q is an integer equal to or larger than 1. For example, the order q is a prime number or a power of a prime number. In other words, the finite field F_q is a prime field or an extended field of the prime field, for example. When the finite field F_q is a prime field, remainder calculations to modulus q can be easily performed, for example. When the finite field F_q is an extended field, remainder calculations modulo an irreducible polynomial can be easily performed, for example. A specific method for configuring a finite field F_q is disclosed, for example, in reference literature 1 "ISO/IEC 18033-2: Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers".
0_F: Additive unit element of the finite field F_q
1_F: Multiplicative unit element of the finite field F_q
δ (i, j): Kronecker's delta function. When i = j, $\delta(i, j) = 1_F$. When $i \neq j$, $\delta(i, j) = 0_F$.

[0049] E: Elliptic curve defined on the finite field F_q. It is defined as a special point O called the point of infinity plus a set of points (x, y) satisfying x, y $\in$ F_q and the Weierstrass equation in an affine coordinate system

$$y^2 + a_1 \cdot x \cdot y + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in F_q$. A binary operation + called an elliptic addition can be defined for any two points on the elliptic curve E, and a unary operation - called an elliptic inverse can be defined for any one point on the elliptic curve E. It is well known that a finite set of rational points on the elliptic curve E forms a group with respect to the elliptic addition. It is also well known that an operation called an elliptic scalar multiplication can be defined with the elliptic addition. A specific operation method of elliptic operations such as the elliptic addition on a computer is also well known. (For example, see reference literature 1; reference literature 2 "RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems"; and reference literature 3 "Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, "Elliptic Curves in Cryptography", Pearson Education, ISBN 4-89471-431-0".)
A finite set of rational points on the elliptic curve E has a subgroup of order p ($p \geq 1$). When the number of elements in a finite set of rational points on the elliptic curve E is #E and p is a large prime number that can divide #E without a remainder, for example, a finite set E[p] of p equally divided points on the elliptic curve E forms a subgroup of a finite set of rational points on the elliptic curve E. The p equally divided points on the elliptic curve E are points A on the elliptic curve E which satisfy the elliptic scalar multiplication $p \cdot A = O$.

[0050] G_1, G_2, G_T: Cyclic groups of order q. Specific examples of the cyclic groups G_1 and G_2 include the finite set E[p] of p equally divided points on the elliptic curve E and subgroups thereof. G_1 may equal G_2, or G_1 may not equal G_2. Specific examples of the cyclic group G_T include a finite set constituting an extended field of the finite field F_q. An example thereof is a finite set of the p-th root of 1 in the algebraic closure of the finite field F_q. Security is enhanced by making the orders of the cyclic groups G_1, G_2, and G_T identical with the order of the finite field F_q.
In the present embodiment, operations defined on the cyclic groups G_1 and G_2 are expressed as additions, and an operation defined on the cyclic group G_T is expressed as a multiplication. More specifically, $\chi \cdot Q \in G_1$ for $\chi \in F_q$ and $\Omega \in G_1$ means that the operation defined in the cyclic group G_1 is applied to $\Omega \in G_1$ χ times, and $\Omega_1 + \Omega_2 \in G_1$ for Ω_1, $\Omega_2 \in G_1$ means that the operation defined in the cyclic group G_1 is applied to $\Omega 1 \in G_1$ and $\Omega_2 \in G_1$. In the same way, $\chi \cdot Q \in G_2$ for $\chi \in F_q$ and $\Omega \in G_2$ means that the operation defined in the cyclic group G_2 is applied to $\Omega \in G_2$ χ times, and $\Omega_1 + \Omega_2 \in G_2$ for $\Omega_1, \Omega_2 \in G_2$ means that the operation defined in the cyclic group G_2 is applied to $\Omega_1 \in G_2$ and $\Omega_2 \in G_2$. In contrast, $\Omega^{\chi} \in G_T$ for $\chi \in F_q$ and $\Omega \in G_T$ means that the operation defined in the cyclic group G_T is applied to $\Omega \in G_T$ χ times, and $\Omega_1 \cdot \Omega_2 \in G_T$ for $\Omega_1, \Omega_2 \in G_T$ means that the operation defined in the cyclic group G_T is applied

to $\Omega_1 \in G_T$ and $\Omega_2 \in G_T$.

[0051] Ψ: Integer equal to or larger than 1

ψ: Integer equal to or larger than 0 and equal to or smaller than Ψ. $\psi = 0, ..., \Psi$.

λ: Integer equal to or larger than 1 and equal to or smaller than Ψ. $\lambda = 1, ..., \Psi$.

$n(\psi)$: Integer equal to or larger than 1

$\zeta(\psi)$: Integer equal to or larger than 0

$G_1^{n(\psi)+\zeta(\psi)}$: Direct product of $(n(\psi) + \zeta(\psi))$ cyclic groups G_1

$G_2^{n(\psi)+\zeta(\psi)}$: Direct product of $(n(\psi) + \zeta(\psi))$ cyclic groups G_2

g_1, g_2, g_T: Generating elements of the cyclic groups G, G_1, G_2, G_T

$V(\psi)$: $(n(\psi) + \zeta(\psi))$-dimensional vector space formed of the direct product of the $(n(\psi) + \zeta(\psi))$ cyclic groups G_1

$V^*(\psi)$: $(n(\psi) + \zeta(\psi))$-dimensional vector space formed of the direct product of the $(n(\psi) + \zeta(\psi))$ cyclic groups G_2

[0052] e_ψ: Non-degenerate bilinear map that maps the direct product $G_1^{n(\psi)+\zeta(\psi)} \times G_2^{n(\psi)+\zeta(\psi)}$ of the direct product $G_1^{n(\psi)+\zeta(\psi)}$ and the direct product $G_2^{n(\psi)+\zeta(\psi)}$ to the cyclic group G_T. The bilinear map e_ψ receives $(n(\psi) + \zeta(\psi))$ elements γ_β ($\beta = 1, ..., n(\psi) + \zeta(\psi)$) of the cyclic group G_1 and $(n(\psi) + \zeta(\psi))$ elements γ_β^* ($\beta = 1, ..., n(\psi) + \zeta(\psi)$) of the cyclic group G_2 and outputs one element of the cyclic group G_T.

$$e_\psi: G_1^{n(\psi)+\zeta(\psi)} \times G_2^{n(\psi)+\zeta(\psi)} \rightarrow G_T \qquad ... (1)$$

[0053] The bilinear map e_ψ satisfies the following characteristics.

- Bilinearity: The following relationship is satisfied for all $T_1 \in G_1^{n(\psi)+\zeta(\psi)}$, $\Gamma_2 \in G_2^{n(\psi)+\zeta(\psi)}$, and $\nu, \kappa \in F_q$.

$$e_\psi(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e_\psi(\Gamma_1, \Gamma_2)^{\nu \cdot \kappa} \qquad ... (2)$$

- Non-degeneracy: This map does not map all $\Gamma_1 \in G_1^{n(\psi)+\zeta(\psi)}$, $\Gamma_2 \in G_2^{n(\psi)+\zeta(\psi)}$ onto the unit element of the cyclic group G_T.
- Computability: There exists an algorithm for efficiently calculating $e_\psi(\Gamma_1, \Gamma_2)$ for all

$$\Gamma_1 \in G_1^{n(\psi)+\zeta(\psi)}, \Gamma_2 \in G_2^{n(\psi)+\zeta(\psi)} \qquad ... (3)$$

[0054] In the present embodiment, the following non-degenerate bilinear map that maps the direct product $G_1 \times G_2$ of the cyclic group G_1 and the cyclic group G_2 to the cyclic group G_T constitutes the bilinear map e_ψ.

$$\text{Pair}: G_1 \times G_2 \rightarrow G_T \qquad ... (4)$$

The bilinear map e_ψ of the present embodiment receives an $(n(\psi) + \zeta(\psi))$-dimensional vector $(\gamma_1, ..., \gamma_{n(\psi)+\zeta(\psi)})$ formed of $(n(\psi) + \zeta(\psi))$ elements γ_β ($\beta = 1, ..., n(\psi) + \zeta(\psi)$) of the cyclic group G_1 and an $(n(\psi) + \zeta(\psi))$-dimensional vector $(\gamma_1^*, ..., \gamma_{n(\psi)+\zeta(\psi)}^*)$ formed of $(n(\psi) + \zeta(\psi))$ elements γ_β^* ($\beta = 1, ..., n(\psi) + \zeta(\psi)$) of the cyclic group G_2 and outputs one element of the cyclic group G_T.

$$e_\psi: \prod_{\beta=1}^{n(\psi)+\zeta(\psi)} \text{Pair}(\gamma_\beta, \gamma_\beta^*) \qquad ... (5)$$

[0055] The bilinear map Pair receives a combination of one element of the cyclic group G_1 and one element of the cyclic group G_2 and outputs one element of the cyclic group G_T. The bilinear map Pair satisfies the following characteristics.

- Bilinearity: The following relationship is satisfied for all $\Omega_1 \in G_1$, $\Omega_2 \in G_2$, and $\nu, \kappa \in F_q$.

$$\text{Pair}(\nu \cdot \Omega_1, \kappa \cdot \Omega_2) = \text{Pair}(\Omega_1, \Omega_2)^{\nu \cdot \kappa} \qquad ... (6)$$

- Non-degeneracy: This map does not map all

$$\Omega_1 \in G_1, \Omega_2 \in G_2 \qquad \ldots (7)$$

onto the unit element of the cyclic group G_T.

- Computability: There exists an algorithm for efficiently calculating Pair(Ω_1, Ω_2) for all $\Omega_1 \in G_1$, $\Omega_2 \in G_2$.
A specific example of the bilinear map Pair is a function for performing a pairing operation such as Weil pairing or Tate pairing. (For example, see reference literature 4 "Alfred. J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, ISBN 0-7923-9368-6, pp. 61-81".) A modified pairing function e(Ω_1, phi(Ω_2)) ($\Omega_1 \in G_1$, $\Omega_2 \in G_2$) obtained by combining a function for performing a pairing operation, such as Tate pairing, and a predetermined function phi according to the type of the elliptic curve E may be used as the bilinear map Pair (for example, see reference literature 2). As the algorithm for performing a pairing operation on a computer, the Miller algorithm (see reference literature 5 "V. S. Miller, "Short Programs for Functions on Curves", 1986, http://crypto.stanford.edu/miller/miller.pdf") or some other known algorithm can be used. Methods for configuring a cyclic group and an elliptic curve used to efficiently perform a pairing operation have been well known. (For example, see reference literature 2; reference literature 6 "A. Miyaji, M. Nakabayashi, and S. Takano, "New Explicit Conditions of Elliptic Curve Traces for FR Reduction", IEICE Trans. Fundamentals, Vol. E84-A, No. 5, pp. 1234-1243, May 2001"; reference literature 7 "P. S. L. M. Barreto, B. Lynn, M. Scott, "Constructing Elliptic Curves with Prescribed Embedding Degrees", Proc. SCN '2002, LNCS 2576, pp. 257-267, Springer-Verlag. 2003"; and reference literature 8 "R. Dupont, A. Enge, F. Morain, "Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields", http://eprint.iacr.org/2002/094/").

[0056] $a_i(\psi)$ ($i = 1, \ldots, n(\psi) + \zeta(\psi)$): $(n(\psi) + \zeta(\psi))$-dimensional basis vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_1 as elements. An example of the basis vector $a_i(\psi)$ is an $(n(\psi) + \zeta(\psi))$-dimensional basis vector having $\kappa_1 \cdot g_1 \in G_1$ as an i-dimensional element and the unit element (expressed as "0" in additive expression) of the cyclic group G_1 as the remaining $(n(\psi) + \zeta(\psi) - 1)$ elements. In that case, each element of the $(n(\psi) + \zeta(\psi))$-dimensional basis vector $a_i(\psi)$ ($i = 1, \ldots, n(\psi) + \zeta(\psi)$) can be listed as follows.

$$\begin{aligned} a_1(\psi) &= (\kappa_1 \cdot g_1, 0, 0, \ldots, 0) \\ a_2(\psi) &= (0, \kappa_1 \cdot g_1, 0, \ldots, 0) \qquad \ldots (8) \\ &\ldots\ldots \\ a_{n(\psi)+\zeta(\psi)}(\psi) &= (0, 0, 0, \ldots, \kappa_1 \cdot g_1) \end{aligned}$$

Here, κ_1 is a constant formed of the elements of the finite field F_q other than the additive unit element 0_F. A specific example of $\kappa_1 \in F_q$ is $\kappa_1 = 1_F$. The basis vector $a_i(\psi)$ is an orthogonal basis. Each $(n(\psi) + \zeta(\psi))$-dimensional vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_1 as elements is expressed by a linear sum of $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $a_i(\psi)$ ($i = 1, \ldots, n(\psi) + \zeta(\psi)$). Therefore, the $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $a_i(\psi)$ span the vector space $V(\psi)$, described earlier.

[0057] $a_i^*(\psi)$ ($i = 1, \ldots, n(\psi) + \zeta(\psi)$): $(n(\psi) + \zeta(\psi))$-dimensional basis vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_2 as elements. An example of the basis vector $a_i^*(\psi)$ is an $(n(\psi) + \zeta(\psi))$-dimensional basis vector having $\kappa_2 \cdot g_2 \in G_2$ as an i-dimensional element and the unit element (expressed as "0" in additive expression) of the cyclic group G_2 as the remaining $(n(\psi) + \zeta(\psi) - 1)$ elements. In that case, each element of the $(n(\psi) + \zeta(\psi))$-dimensional basis vector $a_i^*(\psi)$ ($i = 1, \ldots, n(\psi) + \zeta(\psi)$) can be listed as follows.

$$a_1^*(\psi) = (\kappa_2 \cdot g_2, 0, 0, ..., 0)$$

$$a_2^*(\psi) = (0, \kappa_2 \cdot g_2, 0, ..., 0) \qquad ... (9)$$

.....

$$a_{n(\psi)+\zeta(\psi)}^*(\psi) = (0, 0, 0, ..., \kappa_2 \cdot g_2)$$

Here, κ_2 is a constant formed of the elements of the finite field F_q other than the additive unit element 0_F. A specific example of $\kappa_2 \in F_q$ is $\kappa_2 = 1_F$. The basis vector $a_i^*(\psi)$ is an orthogonal basis. Each $(n(\psi) + \zeta(\psi))$-dimensional vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_2 as elements is expressed by a linear sum of $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $a_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$. Therefore, the $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $a_i^*(\psi)$ span the vector space $V^*(\psi)$, described earlier.

The basis vector $a_i(\psi)$ and the basis vector $a_i^*(\psi)$ satisfy the following expression for the elements $\tau = \kappa_1 \cdot \kappa_2$ of the finite field F_q other than 0_F.

$$e_\psi(a_i(\psi), a_j^*(\psi)) = g_T^{\tau \cdot \delta(i, j)} \qquad ... (10)$$

When i = j, the following expression is satisfied from Expressions (5) and (6).

$$\begin{aligned} e_\psi(a_i(\psi), a_j^*(\psi)) &= \mathrm{Pair}(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2) \cdot \mathrm{Pair}(0, 0) \cdot ... \cdot \mathrm{Pair}(0, 0) \\ &= \mathrm{Pair}(g_1, g_2)^{\kappa 1 \cdot \kappa 2} \cdot \mathrm{Pair}(g_1, g_2)^{0 \cdot 0} \cdot ... \cdot \mathrm{Pair}(g_1, g_2)^{0 \cdot 0} \\ &= \mathrm{Pair}(g_1, g_2)^{\kappa 1 \cdot \kappa 2} = g_T^{\tau} \end{aligned}$$

Here, superscripts κ_1 and κ_2 respectively represent κ_1 and κ_2. When $i \neq j$, the right side of $e_\psi(a_i(\psi), a_j^*(\psi)) = \Pi_{i=1}^{n(\psi)+\zeta(\psi)} \mathrm{Pair}(a_i(\psi), a_j^*(\psi))$ does not include $\mathrm{Pair}(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2)$ and is the product of $\mathrm{Pair}(\kappa_1 \cdot g_1, 0)$, $\mathrm{Pair}(0, \kappa_2 \cdot g_2)$, and $\mathrm{Pair}(0, 0)$. In addition, $\mathrm{Pair}(g_1, 0) = \mathrm{Pair}(0, g_2) = \mathrm{Pair}(g_1, g_2)^0$ is satisfied from Expression (6). Therefore, when $i \neq j$, the following expression is satisfied.

$$e_\psi(a_i(\psi), a_j^*(\psi)) = e_\psi(g_1, g_2)^0 = g_T^0$$

Especially when $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (for example, $\kappa_1 = \kappa_2 = 1_F$), the following expression is satisfied.

$$e(a_i(\psi), a_j^*(\psi)) = g_T^{\delta(i, j)} \qquad ... (11)$$

Here, $g_T^0 = 1$ is the unit element of the cyclic group G_T, and $g_T^1 = g_T$ is a generating element of the cyclic group G_T. In that case, the basis vector $a_i(\psi)$ and the basis vector $a_i^*(\psi)$ are a dual normal orthogonal basis, and the vector space $V(\psi)$ and the vector space $V^*(\psi)$ are a dual vector space that can constitute bilinear mapping (dual pairing vector space (DPVS)).

[0058] $A(\psi)$: An $(n(\psi) + \zeta(\psi))$ row by $(n(\psi) + \zeta(\psi))$ column matrix having the basis vector $a_i(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ as elements. When the basis vector $a_i(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ is expressed by Expression (8), for example, the matrix $A(\psi)$ is as follows.

$$A(\psi) = \begin{pmatrix} a_1(\psi) \\ a_2(\psi) \\ \vdots \\ a_{n(\psi)+\zeta(\psi)}(\psi) \end{pmatrix} = \begin{pmatrix} \kappa_1 \cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1 \cdot g_1 \end{pmatrix} \quad \cdots (12)$$

[0059] $A^*(\psi)$: An $(n(\psi) + \zeta(\psi))$ row by $(n(\psi) + \zeta(\psi))$ column matrix having the basis vector $a_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ as elements. When the basis vector $a_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ is expressed by Expression (9), for example, the matrix $A^*(\psi)$ is as follows.

$$A^*(\psi) = \begin{pmatrix} a_1^*(\psi) \\ a_2^*(\psi) \\ \vdots \\ a_{n(\psi)+\zeta(\psi)}^*(\psi) \end{pmatrix} = \begin{pmatrix} \kappa_2 \cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2 \cdot g_2 \end{pmatrix} \cdots (13)$$

[0060] $X(\psi)$: An $(n(\psi) + \zeta(\psi))$ row by $(n(\psi) + \zeta(\psi))$ column matrix having elements of the finite field F_q as elements. The matrix $X(\psi)$ is used to apply coordinate conversion to the basis vector $a_i(\psi)$. When the element located at the i-th row and the j-th column $(i = 1, ..., n(\psi) + \zeta(\psi), j = 1, ..., n(\psi) + \zeta(\psi))$ in the matrix $X(\psi)$ is $\chi_{i,j}(\psi) \in F_q$, the matrix $X(\psi)$ is as follows.

$$X(\psi) = \begin{pmatrix} \chi_{1,1}(\psi) & \chi_{1,2}(\psi) & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}(\psi) \\ \chi_{2,1}(\psi) & \chi_{2,2}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}(\psi) & \chi_{n(\psi)+\zeta(\psi),2}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}(\psi) \end{pmatrix} \cdots (14)$$

Here, each element $\chi(\psi)$ of the matrix $X(\psi)$ is called a conversion coefficient.

[0061] $X^*(\psi)$: $X^*(\psi)$ and the matrix $X(\psi)$ satisfy the relationship of $X^*(\psi) = \tau' \cdot (X(\psi)^{-1})^T$. Note that $\tau' \in F_q$ is an arbitrary constant belonging to the finite field F_q, and $\tau' = 1_F$, for example. The matrix $X^*(\psi)$ is used to apply coordinate conversion to the basis vector $a_i^*(\psi)$. When the element located at the i-th row and the j-th column in the matrix $X^*(\psi)$ is $\chi_{i,j}^*(\psi) \in F_q$, the matrix $X^*(\psi)$ is as follows.

$$X^*(\psi) = \begin{pmatrix} \chi_{1,1}^*(\psi) & \chi_{1,2}^*(\psi) & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}^*(\psi) \\ \chi_{2,1}^*(\psi) & \chi_{2,2}^*(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}^*(\psi) & \chi_{n(\psi)+\zeta(\psi),2}^* & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}^* \end{pmatrix} \cdots (15)$$

Here, each element $\chi_{i,j}^*(\psi)$ of the matrix $X^*(\psi)$ is called a conversion coefficient.

In that case, when an $(n(\psi) + \zeta(\psi))$ row by $(n(\psi) + \zeta(\psi))$ column unit matrix is $I(\psi)$, $X(\psi) \cdot (X^*(\psi) = \tau' \cdot I(\psi)$. In other words, for the unit matrix given below,

$$I(\psi) = \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \cdots (16)$$

the following expression is satisfied.

$$\begin{pmatrix} \chi_{1,1}(\psi) & \chi_{1,2}(\psi) & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}(\psi) \\ \chi_{2,1}(\psi) & \chi_{2,2}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}(\psi) & \chi_{n(\psi)+\zeta(\psi),2}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta}(\psi) \end{pmatrix}$$

$$\times \begin{pmatrix} \chi_{1,1}^{*}(\psi) & \chi_{2,1}^{*}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),1}^{*}(\psi) \\ \chi_{1,2}^{*}(\psi) & \chi_{2,2}^{*}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n(\psi)+\zeta(\psi)}^{*}(\psi) & \chi_{2,n(\psi)+\zeta(\psi)}^{*}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}^{*}(\psi) \end{pmatrix}$$

$$= \tau' \cdot \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \qquad \cdots (17)$$

Here, $(n(\psi) + \zeta(\psi))$-dimensional vectors will be defined below.

$$\chi_i^{\rightarrow}(\psi) = (\chi_{i,1}(\psi), \ldots, \chi_{i,n(\psi)+\zeta(\psi)}(\psi)) \qquad \ldots (18)$$

$$\chi_j^{\rightarrow *}(\psi) = (\chi_{j,1}^{*}(\psi), \ldots, \chi_{j,n(\psi)+\zeta(\psi)}^{*}(\psi)) \qquad \ldots (19)$$

The inner product of the $(n(\psi) + \zeta(\psi))$-dimensional vectors $\chi_i^{\rightarrow}(\psi)$ and $\chi_j^{\rightarrow *}(\psi)$ satisfies the following expression from Expression (17).

$$\chi_i^{\rightarrow}(\psi) \cdot \chi_j^{\rightarrow *}(\psi) = \tau' \cdot \delta(i, j) \qquad \ldots (20)$$

[0062] $b_i(\psi)$: $(n(\psi) + \zeta(\psi))$-dimensional basis vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_1 as elements. The basis vector $b_i(\psi)$ is obtained by applying coordinate conversion to the basis vector $a_i(\psi)$ $(i = 1, \ldots, n(\psi) + \zeta(\psi))$ by using the matrix $X(\psi)$. Specifically, the basis vector $b_i(\psi)$ is obtained by the following calculation.

$$b_i(\psi) = \sum_{j=1}^{n(\psi)+\zeta(\psi)} \chi_{i,j}(\psi) \cdot a_j(\psi) \qquad \ldots (21)$$

For example, when the basis vector $a_j(\psi)$ $(j = 1, \ldots, n(\psi) + \zeta(\psi))$ is expressed by Expression (8), each element of the basis vector $b_i(\psi)$ can be listed as follows.

$$b_i(\psi) = (\chi_{i,1}(\psi) \cdot \kappa_1 \cdot g_1, \chi_{i,2}(\psi) \cdot \kappa_1 \cdot g_1, \ldots, \chi_{i,n(\psi)+\zeta(\psi)}(\psi) \cdot \kappa_1 \cdot g_1) \qquad \ldots (22)$$

Each $(n(\psi) + \zeta(\psi))$-dimensional vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_1 as elements is expressed by a linear sum of $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $b_i(\psi)$ $(i = 1, \ldots, n(\psi) + \zeta(\psi))$. Therefore, the $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $b_i(\psi)$ span the vector space $V(\psi)$, described earlier.

[0063] $b_i^*(\psi)$: $(n(\psi) + \zeta(\psi))$-dimensional basis vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_2 as elements. The basis vector $b_i^*(\psi)$ is obtained by applying coordinate conversion to the basis vector $a_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ by using the matrix $X^*(\psi)$. Specifically, the basis vector $b_i^*(\psi)$ is obtained by the following calculation.

$$b_i^*(\psi) = \sum_{j=1}^{n(\psi)+\zeta(\psi)} \chi_{i,j}^*(\psi) \cdot a_j^*(\psi) \qquad ... (23)$$

For example, when the basis vector $a_j^*(\psi)$ $(j = 1, ..., n(\psi) + \zeta(\psi))$ is expressed by Expression (9), each element of the basis vector $b_i^*(\psi)$ can be listed as follows.

$$b_i^*(\psi) = (\chi_{i,1}^*(\psi) \cdot \kappa_2 \cdot g_2, \chi_{i,2}^*(\psi) \cdot \kappa_2 \cdot g_2, ..., \chi_{i,n(\psi)+\zeta(\psi)}^*(\psi) \cdot \kappa_2 \cdot g_2) \qquad ... (24)$$

Each $(n(\psi) + \zeta(\psi))$-dimensional vector having $(n(\psi) + \zeta(\psi))$ elements of the cyclic group G_2 as elements is expressed by a linear sum of $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $b_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$. Therefore, the $(n(\psi) + \zeta(\psi))$-dimensional basis vectors $b_i^*(\psi)$ span the vector space $V^*(\psi)$, described earlier.
The basis vector $b_i(\psi)$ and the basis vector $b_i^*(\psi)$ satisfy the following expression for the elements $\tau = \kappa_1 \cdot \kappa_2$ of the finite field F_q other than 0_F.

$$e_\psi(b_i(\psi), b_j^*(\psi)) = g_T^{\tau \cdot \tau' \cdot \delta(i,j)} \qquad .... (25)$$

The following expression is satisfied from Expressions (5), (20), (22), and (24).

$$\begin{aligned} e_\psi(b_i(\psi), b_j^*(\psi)) &= \prod_{\beta=1}^{n(\psi)+\zeta(\psi)} \mathrm{Pair}(\chi_{i,\beta}(\psi) \cdot \kappa_1 \cdot g_1, \chi_{j,\beta}^*(\psi) \cdot \kappa_2 \cdot g_2) \\ &= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \vec{\chi_i}(\psi) \cdot \vec{\chi_j}^*(\psi)} \\ &= \mathrm{Pair}(g_1, g_2)^{\tau \cdot \tau' \cdot \delta(i,j)} = g_T^{\tau \cdot \tau' \cdot \delta(i,j)} \end{aligned}$$

Especially when $\kappa = \kappa_1 \cdot \kappa_2 = 1_F$ (for example, $\kappa_1 = \kappa_2 = 1_F$), the following expression is satisfied.

$$e_\psi(b_i(\psi), b_j^*(\psi)) = g_T^{\delta(i,j)} \qquad ... (26)$$

In that case, the basis vector $b_i(\psi)$ and the basis vector $b_i^*(\psi)$ are the dual normal orthogonal basis of a dual pairing vector space (the vector space $V(\psi)$ and the vector space $V^*(\psi)$).
As long as Expression (25) is satisfied, the basis vectors $a_i(\psi)$ and $a_i^*(\psi)$ other than those shown in Expressions (8) and (9) as examples and the basis vectors $b_i(\psi)$ and $b_i^*(\psi)$ other than those shown in Expressions (21) and (23) as examples may be used.
[0064] $B(\psi)$: An $(n(\psi) + \zeta(\psi))$ row by $(n(\psi) + \zeta(\psi))$ column matrix having the basis vector $b_i(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ as elements. $B(\psi) = X(\psi) \cdot A(\psi)$ is satisfied. For example, when the basis vector $b_i(\psi)$ is expressed by Expression (22), the matrix $B(\psi)$ is as follows.

$$B(\psi) = \begin{pmatrix} b_1(\psi) \\ b_2(\psi) \\ \vdots \\ b_{n(\psi)+\zeta(\psi)}(\psi) \end{pmatrix} = \begin{pmatrix} \chi_{1,1}(\psi)\cdot\kappa_1\cdot g_1 & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}(\psi)\cdot\kappa_1\cdot g_1 \\ \vdots & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}(\psi)\cdot\kappa_1\cdot g_1 & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}\cdot\kappa_1\cdot g_1 \end{pmatrix} \quad \cdots (27)$$

[0065] $B^*(\psi)$: An $(n(\psi) + \zeta(\psi))$ row by $(n(\psi) + \zeta(\psi))$ column matrix having the basis vector $b_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ as elements. $B^*(\psi) = X^*(\psi) \cdot A^*(\psi)$ is satisfied. For example, when the basis vector $b_i^*(\psi)$ $(i = 1, ..., n(\psi) + \zeta(\psi))$ is expressed by Expression (24), the matrix $B^*(\psi)$ is as follows.

$$B^*(\psi) = \begin{pmatrix} b_1^*(\psi) \\ b_2^*(\psi) \\ \vdots \\ b_{n(\psi)+\zeta(\psi)}^*(\psi) \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^*(\psi)\cdot\kappa_2\cdot g_2 & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}^*(\psi)\cdot\kappa_2\cdot g_2 \\ \vdots & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}^*(\psi)\cdot\kappa_2\cdot g_2 & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}^*(\psi)\cdot\kappa_2\cdot g_2 \end{pmatrix} \quad \cdots (28)$$

[0066] $v(\lambda)^{\rightarrow}$: An $n(\lambda)$-dimensional vector having elements of the finite field F_q as elements.

$$v(\lambda)^{\rightarrow} = (v_1(\lambda), ..., v_{n(\lambda)}(\lambda)) \in F_q^{n(\lambda)} \quad ... (29)$$

$v_\mu(\lambda)$: The μ-th $(\mu = 1, ..., n(\lambda))$ element of the $n(\lambda)$-dimensional vector $v(\lambda)^{\rightarrow}$.
$w(\lambda)^{\rightarrow}$: An $n(\lambda)$-dimensional vector having elements of the finite field F_q as elements.

$$w(\lambda)^{\rightarrow} = (w_1(\lambda), ..., w_{n(\lambda)}(\lambda)) \in F_q^{n(\lambda)} \quad ... (30)$$

$w_\mu(\lambda)$: The μ-th $(\mu = 1, ..., n(\lambda))$ element of the $n(\lambda)$-dimensional vector $w(\lambda)^{\rightarrow}$.
Enc: A common key encryption function that indicates an encryption process of a common key cryptosystem.
$Enc_k(M)$: Ciphertext obtained by encrypting plaintext M by the common key encryption function Enc with the use of a common key K.
Dec: A common key decryption function that indicates a decryption process of the common key cryptosystem.
$Dec_k(C)$: A decryption result obtained by decrypting ciphertext C by the common key decryption function Dec with the use of the common key K.

[Function Cryptosystem]

[0067] Next, the basic configuration of function cryptosystem will be described below.
In the function cryptosystem, a ciphertext is decoded in the case where the true value of a logical expression determined

by the combination of first information and second information is "true". One of the "first information" and the "second information" is embedded in the ciphertext, and the other thereof is embedded in key information. For example, a predicate cryptosystem disclosed in ""Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products", with Amit Sahai and Brent Waters One of 4 papers from Eurocrypt 2008 invited to the Journal of Cryptology" (reference literature 9) is one of function cryptosystems.

[0068] There exist various known function cryptosystems other than the one given above, and a new function cryptosystem that has not been published is described below. In the new function cryptosystem to be described below, secrets of a value according to secret information are hierarchically shared in a mode according to a predetermined logical expression. The predetermined logical expression includes a propositional variable whose true value is determined by the combination of the first information and the second information, and further includes all or some of the logical symbols $\wedge$, $\vee$, and $\neg$ as needed. Then, in the case where the true value of the predetermined logical expression, which is determined by identifying the true value of each propositional variable, is "true", the value according to the secret information is restored, and the ciphertext is decrypted on the basis of the restored value.

<Relationship between Logical Expression and Hierarchical Secret Sharing>

[0069] The relationship between the predetermined logical expression and the hierarchical secret sharing will be described.

The secret sharing refers to dividing secret information into N ($N \geq 2$) pieces of share information such that the secret information is restored only in the case where K_t ($K_t \geq 1$) or more pieces (threshold value) of share information are obtained. A secret sharing scheme (SSS) that satisfies $K_t = N$ is called an N-out-of-N sharing scheme (or "N-out-of-N threshold sharing scheme"), and a secret sharing scheme that satisfies $K_t < N$ is called a K_t-out-of-N sharing scheme (or "K_t-out-of-N threshold sharing scheme") (for example, see reference literature 10 "Kaoru Kurosawa, Wakaha Ogata "Basic Mathematics of Modern Cryptography (IEICE Lecture Series)", Corona Publishing Co., Ltd., March 2004, p. 116-119"; and reference literature 11 "A. Shamir, "How to Share a Secret", Communications of the ACM, November 1979, Volume 22, Number 11, pp. 612-613.").

[0070] In the N-out-of-N sharing scheme, if all pieces of share information share(1), ..., share(N) are given, secret information SE can be restored, but even if (N - 1) pieces of arbitrary share information share(φ_1), ..., share(φ_{N-1}) are given, the secret information SE cannot be obtained at all. An example thereof is given below.

- SH, ..., SH_{N-1} are randomly selected.
- Calculation of $SH_N = SE - (SH_1 + ... + SH_{N-1})$ is performed.
- SH_1, ..., SH_N are respectively defined as the pieces of share information share(1), ..., share(N).
- If all the pieces of share information share(1), ..., share(N) are given, the secret information SE can be restored by a restoration process using the following expression.

$$SE = share(1) + ... + share(N) \qquad ... (31)$$

[0071] In the K_t-out-of-N sharing scheme, if K_t pieces of arbitrary different share information share(φ1), ..., share(φ_{Kt}) are given, the secret information SE can be restored, but even if (K_t - 1) pieces of arbitrary share information share (φ_1), ..., share(φ_{Kt-1}) are given, the secret information SE cannot be obtained at all. Note that the subscript Kt represents K_t. An example of the K_t-out-of-N sharing scheme is given below.

[0072] • A (K_t - 1)-order polynomial $f(x) = \xi_0 + \xi_1 \cdot x + \xi_2 \cdot x^2 + ... + \xi_{Kt-1} \cdot x^{Kt-1}$ that satisfies f(0) = SE is randomly selected. That is, assuming that $\xi_0 = SE$, ξ_1, ..., ξ_{Kt-1} are randomly selected. The share information is defined as share (ρ) = (ρ, f(ρ)) (ρ = 1, ..., N). Note that (ρ, f(ρ)) is information that can extract values of p and f(p), and is a bit connecting value of ρ and f(ρ), for example.

[0073] • In the case where K_t pieces of arbitrary different share information share(φ_1), ..., share(φ_{Kt}) ((φ_1, ..., φ_{Kt}) $\subset$ (1, ..., N)) are obtained, for example, the secret information SE can be restored by a restoration process using the following expression, according to the Lagrange formula for interpolation.

$$SE = f(0) = LA_1 \cdot f(\varphi_1) + ... + LA_{Kt} \cdot f(\varphi_{Kt}) \qquad ... (32)$$

$$LA_{\rho}(x) = \frac{(x-\phi_1)\cdots\overset{\rho}{\vee}\cdots(x-\phi_{K_t})}{(\phi_{\rho}-\phi_1)\cdots\overset{\rho}{\vee}\cdots(\phi_{\rho}-\phi_{K_t})} \in F_q \qquad \cdots(33)$$

where ==========
means that a ρ-th operand from the beginning, which has a denominator element (φ_{ρ} - φ_{ρ}) and a numerator element (x - φ_{ρ}), does not exist. That is, the denominator of Expression (33) is as follows.

$$(\varphi_{\rho} - \varphi_1) \cdot \ldots \cdot (\varphi_{\rho} - \varphi_{\rho-1}) \cdot (\varphi_{\rho} - \varphi_{\rho+1}) \cdot \ldots \cdot (\varphi_{\rho} - \varphi_{Kt})$$

The numerator of Expression (33) is as follows.

$$(x - \varphi_1) \cdot \ldots \cdot (x - \varphi_{\rho-1}) \cdot (x - \varphi_{\rho+1}) \cdot \ldots \cdot (x - \varphi_{Kt})$$

[0074] Each secret sharing described above can be executed in the field. Further, through extension thereof, secrets of a value according to secret information SE can be shared to pieces of share information share. The value according to the secret information SE refers to the secret information SE itself and a function value of the secret information SE, and the value according to the share information share refers to the share information share itself and a function value of the share information. For example, secrets of elements $g_T^{SE} \in G_T$ of the cyclic group G_T according to the secret information SE $\in F_q$ constituting elements of the finite field F_q can be shared to elements $g_T^{share(1)}$, $g_T^{share(2)} \in G_T$ of the cyclic group G_T according to the pieces of share information share(1), share(2) of the secret information SE. Further, the secret information SE described above is a linear combination of the pieces of share information share (Expressions (31) and (32)). Such a secret sharing scheme in which the secret information SE is a linear combination of the pieces of share information share is called a linear secret sharing scheme.

[0075] The predetermined logical expression described above can be expressed by tree structure data obtained by hierarchically sharing secrets of the secret information. That is, according to De Morgan's laws, the predetermined logical expression described above can be expressed by a logical expression formed of literals or a logical expression formed of at least part of the logical symbols $\wedge$ and $\vee$ and literals (these will be called "standard logical expressions"), and such a standard logical expression can be expressed by tree structure data obtained by hierarchically sharing secrets of the secret information.

[0076] Tree structure data that expresses a standard logical expression includes a plurality of nodes, at least part of the nodes are defined as a parent node of one or more child nodes, one of the parent nodes is defined as a root node, and at least part of the child nodes are defined as a leaf node. A parent node of the root node and a child node of the leaf node do not exist. A value according to secret information corresponds to the root node, and a value according to share information obtained by sharing secrets of a value corresponding to each parent node corresponds to a child node of this parent node. Secret sharing modes (such as a secret sharing scheme and a threshold value) at each node are determined in accordance with a standard logical expression. Further, each literal constituting the standard logical expression corresponds to each leaf node, and the true value of each literal is determined by the combination of the first information and the second information.

[0077] Here, it is assumed that a value according to share information corresponding to a leaf node corresponding to a literal whose true value is "true" can be obtained, whereas a value according to share information corresponding to a leaf node corresponding to a literal whose true value is "false" cannot be obtained. Further, on the basis of the characteristics of the secret sharing described above, a value according to share information corresponding to a parent node (a value according to secret information, if this parent node is the root node) is restored only in the case where a number of values according to share information corresponding to child node(s) of this parent node are obtained, the number being equal to or more than a threshold value corresponding to this parent node. Accordingly, whether or not the value according to the secret information corresponding to the root node can be finally restored is determined in accordance with: the true value of a literal corresponding to which leaf node is "true"; and configurations of the tree structure data (including the secret sharing modes at each node). Then, the tree structure data configured in the following manner expresses a standard logical expression. That is, only in the case where the true value of each literal corresponding to each leaf node makes the true value of the standard logical expression "true", the value according to the secret information corresponding to the root node can be finally restored. Such tree structure data that expresses the standard logical expression can be easily set. A specific example thereof is given below.

[0078] Fig. 83 is a view illustrating tree structure data that expresses a standard logical expression PRO(1)∧PRO(2)∨¬PRO(3) including: propositional variables PRO(1) and PRO(2); a negation ¬PRO(3) of a propositional variable PRO(3); and the logical symbols ∧ and ∨. The tree structure data illustrated in Fig. 83 includes a plurality of nodes N_1, ..., N_5. The node N_1 is the parent node of the nodes N_2 and N_5, the node N_2 is the parent node of the nodes N_3 and N_4, the node N_1 as one of the parent nodes is the root node, and the nodes N_3, N_4, and N_5 as part of the child nodes are the leaf nodes. A value according to secret information SE corresponds to the node N_1, and values according to pieces of share information SE, SE obtained by sharing secrets of the value according to the secret information SE using a 1-out-of-2 sharing scheme respectively correspond to the child nodes N_2 and N_5 of the node N_1. Values according to pieces of share information SE-SH_1, SH_1 obtained by sharing secrets of the value according to the share information SE using a 2-out-of-2 sharing scheme respectively correspond to the child nodes N_3 and N_4 of the node N_2. That is, the value according to the share information share(1) = SE-SH_1 corresponds to the leaf node N_3, the value according to the share information share(2) = SH_1 corresponds to the leaf node N_4, and the value according to the share information share(3) = SE corresponds to the leaf node N_5. Further, the literals PRO(1), PRO(2), and ¬PRO(3) constituting the standard logical expression PRO(1)∧PRO(2)∨¬PRO(3) respectively correspond to the leaf nodes N_3, N_4, and N_5, and the true values of the literals PRO(1), PRO(2), and ¬PRO(3) are determined by the combination of the first information and the second information. Here, a value according to share information corresponding to a leaf node corresponding to a literal whose true value is "true" can be obtained, whereas a value according to share information corresponding to a leaf node corresponding to a literal whose true value is "false" cannot be obtained. In this case, only in the case where the combination of the first information and the second information makes the true value of the standard logical expression PRO(1)∧PRO(2)∨¬PRO(3) "true", the value according to the secret information SE is restored.

[0079] Fig. 84 is a view illustrating tree structure data that expresses a standard logical expression PRO(1)∧PRO(2)∨PRO(2)∧PRO(3)∨PRO(1)∧PRO(3)∨¬PRO(4)∨(¬PRO(5)∧PRO(6))∧PRO(7) including: propositional variables PRO(1), PRO(2), PRO(3), PRO(6), and PRO(7); negations ¬PRO(4) and ¬PRO(5) of propositional variables PRO(4) and PRO(5); and the logical symbols ∧ and v.

The tree structure data illustrated in Fig. 84 includes a plurality of nodes N_1,..., N_{11}. The node N_1 is the parent node of the nodes N_2, N_6, and N_7, the node N_2 is the parent node of the nodes N_3, N_4, and N_5, the node N_7 is the parent node of the nodes N_8 and N_{11}, the node N_8 is the parent node of the nodes N_9 and N_{10}, the node N_1 as one of the parent nodes is the root node, and the nodes N_3, N_4, N_5, N_6, N_9, N_{10}, and N_{11} are the leaf nodes. A value according to secret information SE corresponds to the node N_1, and values according to pieces of share information SE, SE, SE obtained by sharing secrets of the value according to the secret information SE using a 1-out-of-3 sharing scheme respectively correspond to the child nodes N_2, N_6, and N_7 of the node N_1. Values according to pieces of share information (1, f(1)), (2, f(2)), (3, f(3)) obtained by sharing secrets of the value according to the share information SE using a 2-out-of-3 sharing scheme respectively correspond to the child nodes N_3, N_4, and N_5 of the node N_2. Values according to pieces of share information SH_4, SE-SH_4 obtained by sharing secrets of the value according to the share information SE using a 2-out-of-2 sharing scheme respectively correspond to the child nodes N_8 and N_{11} of the node N_7. Values according to pieces of share information SH_4, SH_4 obtained by sharing secrets of the value according to the share information SH_4 using a 1-out-of-2 sharing scheme respectively correspond to the child nodes N_9 and N_{10} of the node N_8. That is, the value according to the share information share(1) = (1, f(1)) corresponds to the leaf node N_3, the value according to the share information share(2) = (2, f(2)) corresponds to the leaf node N_4, the value according to the share information share(3) = (3, f(3)) corresponds to the leaf node N_5, the value according to the share information share(4) = SE corresponds to the leaf node N_6, the value according to the share information share(5) = SH_4 corresponds to the leaf node N_9, the value according to the share information share(6) = SH_4 corresponds to the leaf node N_{10}, and the value according to the share information share(7) = SE-SH_4 corresponds to the leaf node N_{11}. Further, the literals PRO(1), PRO(2), PRO(2), PRO(3), PRO(1), PRO(3), ¬PRO(4), ¬PRO(5), PRO(6), and PRO(7) constituting the standard logical expression PRO(1)∧PRO(2)∨PRO(2)∧PRO(3)∨PRO(1)∧PRO(3)∨¬PRO(4)∨(¬PRO(5) ∧PRO(6))∧PRO(7) respectively correspond to the leaf nodes N_3, N_4, N_5, N_6, N_9, N_{10}, and N_{11}, and the true values of the literals PRO(1), PRO(2), PRO(2), PRO(3), PRO(1), PRO(3), ¬PRO(4), ¬PRO(5), PRO(6), and PRO(7) are determined by the combination of the first information and the second information. Here, a value according to share information corresponding to a leaf node corresponding to a literal whose true value is "true" can be obtained, whereas a value according to share information corresponding to a leaf node corresponding to a literal whose true value is "false" cannot be obtained. In this case, only in the case where the combination of the first information and the second information makes the true value of the standard logical expression PRO(1), ∧PRO(2), ∨PRO(2), ∧PRO(3), ∨PRO(1), ∧PRO(3), ∨¬PRO(4), ∨(¬PRO(5), ∧PRO(6),)∧PRO(7) "true", the value according to the secret information SE is restored.

<Access Structure>

[0080] In the case as described above where a predetermined logical expression is expressed by tree structure data obtained by hierarchically sharing secrets of secret information, whether the true value of a logical expression determined

by the combination of the first information and the second information is "true" or "false" can be determined depending on whether or not a value according to the secret information can be restored from values according to share information at leaf nodes obtained for the combination of the first information and the second information. Hereinafter, a mechanism is called an access structure, in which: the combination of the first information and the second information is accepted in the case where the true value of the logical expression determined by the combination of the first information and the second information is "true"; and the combination of the first information and the second information is rejected in the case where the true value thereof is "false".

[0081] The total number of leaf nodes of the tree structure data that expresses the predetermined logical expression as described above is defined as Ψ, and identifiers respectively corresponding to the leaf nodes are defined as λ, = 1, ..., Ψ. A set $\{v(\lambda)^{\rightarrow}\}_{\lambda 1, ..., \Psi}$ of n(λ)-dimensional vectors $v(\lambda)^{\rightarrow}$ corresponding to the leaf nodes is defined as the first information, and a set $\{w(\lambda)^{\rightarrow}\}_{\lambda=1, ..., \Psi}$ of n(λ)-dimensional vectors $w(\lambda)^{\rightarrow}$ corresponding to the leaf nodes is defined as the second information. Further, the tree structure data described above is mounted as a labeled matrix LMT (MT, LAB).

[0082] The labeled matrix LMT (MT, LAB) includes a Ψ row by COL (COL $\geq$ 1) column matrix

$$MT = \begin{pmatrix} mt_{1,1} & \cdots & mt_{1,COL} \\ \vdots & \ddots & \vdots \\ mt_{\Psi,1} & \cdots & mt_{\Psi,COL} \end{pmatrix} \quad \cdots (34)$$

and a label LAB(λ) associated with each row λ = 1, ..., Ψ of the matrix MT.

[0083] Each element $mt_{\lambda, col}$ (col = 1, ..., COL) of the matrix MT satisfies the following two requirements. Firstly, in the case where a value according to secret information SE $\in F_q$ corresponds to the root node of the tree structure data that expresses the predetermined logical expression as described above, the following expression (37) is established for the following COL-dimensional vector (35) having elements of a predetermined finite field F_q as elements and the following COL-dimensional vector (36) having elements of a finite field F_q according to the secret information SE as elements.

$$GV^{\rightarrow} = (gv_1, ..., gv_{COL}) \in F_q^{COL} \quad ... (35)$$

$$CV^{\rightarrow} = (cv_1, ..., cv_{COL}) \in F_q^{COL} \quad ... (36)$$

$$SE = GV^{\rightarrow} \cdot (CV^{\rightarrow})^T \quad ... (37)$$

A specific example of the COL-dimensional vector $GV^{\rightarrow}$ is as follows.

$$GV^{\rightarrow} = (1_F, ..., 1_F) \in F_q^{COL} \quad ... (38)$$

The COL-dimensional vector $GV^{\rightarrow}$ may be other COL-dimensional vectors such as $GV^{\rightarrow} = (1_F, 0_F, ..., 0_F) \in F_q^{COL}$. Secondly, in the case where a value according to share information share(λ) $\in F_q$ corresponds to a leaf node corresponding to an identifier λ, the following expression is established.

$$(share(1), ..., share(\Psi))^T = MT \cdot (CV^{\rightarrow})^T \quad ... (39)$$

If the tree structure data that expresses the predetermined logical expression is determined as described above, the matrix MT that satisfies these two requirements is easily selected. Further, even if the secret information SE and the share information share(λ) are variables, the matrix MT that satisfies these two requirements is easily selected. That is, after the determination of the matrix MT, values of the secret information SE and the share information share(λ) may be determined.

[0084] Further, the label LAB(λ) associated with each row λ = 1, ..., Ψ of the matrix MT corresponds to a literal (PRO(λ)

or ¬PRO(λ)) corresponding to a leaf node corresponding to the identifier λ. Here, it is assumed that the following first case is equivalent to the following second case. That is, in the first case, the true value of the propositional variable PRO (λ) is "true". In the second case, the inner product $v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow}$ of $v(\lambda)^{\rightarrow}$ included in first information VSET1 = {λ, $v(\lambda)^{\rightarrow}$ |λ = 1, ..., Ψ} and $w(\lambda)^{\rightarrow}$ included in second information VSET2 = {λ, $w(\lambda)^{\rightarrow}$ |λ = 1, ..., Ψ} is 0. It is also assumed that the following third case is equivalent to the following fourth case. That is, in the third case, the true value of the propositional variable PRO(λ) is "false". In the fourth case, the inner product $v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow}$ is not 0. Then, it is assumed that the label LAB(λ) corresponding to PRO(λ) represents $v(\lambda)^{\rightarrow}$ and that the label LAB(λ) corresponding to ¬PRO(λ) represents $\neg v(\lambda)^{\rightarrow}$. Note that $\neg v(\lambda)^{\rightarrow}$ is a logical expression representing the negation of $v(\lambda)^{\rightarrow}$, and $v(\lambda)^{\rightarrow}$ can be identified from $\neg v(\lambda)^{\rightarrow}$. Further, the case where LAB(λ) represents $v(\lambda)^{\rightarrow}$ is expressed by "LAB(λ) = $v(\lambda)^{\rightarrow}$", and the case where LAB(λ) represents $\neg v(\lambda)^{\rightarrow}$ is expressed by "LAB(λ) = $\neg v(\lambda)^{\rightarrow}$". Further, a set $\{LAB(\lambda)\}_{\lambda=1, ..., \Psi}$ of LAB(λ) (λ = 1, ..., Ψ) is expressed by LAB.

[0085] Moreover, the following Ψ-dimensional vector is defined.

$$TFV^{\rightarrow} = (tfv(1), ..., tfv(\Psi)) \qquad ... (40)$$

An element tfv(λ) is 1 if the inner product $v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow}$ is 0, and the element tfv(λ) is 0 if the inner product $v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow}$ is other than 0.

$$tfv(\lambda) = 1 \ (PRO(\lambda) \text{ is "true"}) \text{ if } v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow} = 0 \qquad ... (41)$$

$$tfv(\lambda) = 0 \ (PRO(\lambda) \text{ is "false"}) \text{ if } v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow} \neq 0 \qquad ... (42)$$

[0086] Moreover, the case where the true value of the following logical expression is "true" is expressed by LIT(λ) = 1.

$$\{(LAB(\lambda) = v(\lambda)^{\rightarrow}) \wedge (tfv(\lambda) = 1)\} \vee \{(LAB(\lambda) = \neg v(\lambda)^{\rightarrow}) \wedge (tfv(\lambda) = 0)\} \qquad ... (43)$$

The case where the true value thereof is "false" is expressed by LIT(λ) = 0. That is, the case where the true value of a literal corresponding to a leaf node corresponding to the identifier λ is "true" is expressed by LIT(λ) = 1, and the case where the true value thereof is "false" is expressed by LIT(λ) = 0. Under the circumstances, a submatrix MT_{TFV} formed of only row vectors $mt_{\lambda}^{\rightarrow} = (mt_{\lambda, 1}, ..., mt_{\lambda, COL})$ whose LIT(λ) is 1, among the row vectors included in the matrix MT, can be expressed as follows.

$$MT_{TFV} = (MT)_{LIT(\lambda)=1} \qquad ... (44)$$

[0087] In the case where the secret sharing scheme described above is a linear secret sharing scheme, the following first case is equivalent to the following second case. That is, in the first case, the value according to the secret information SE can be restored from the value according to the share information share(λ) corresponding to the identifier λ. In the fourth case, the COL-dimensional vector $GV^{\rightarrow}$ belongs to a vector space spanned by the row vectors $mt_{\lambda}^{\rightarrow}$ corresponding to the identifier λ. That is, whether or not the value according to the secret information SE can be restored from the value according to the share information share(λ) corresponding to the identifier λ can be determined by determining whether or not the COL-dimensional vector $GV^{\rightarrow}$ belongs to the vector space spanned by the row vectors $mt_{\lambda}^{\rightarrow}$ corresponding to the identifier λ. Note that the vector space spanned by the row vectors $mt_{\lambda}^{\rightarrow}$ means a vector space that can be represented by the linear combination of the row vectors $mt_{\lambda}^{\rightarrow}$.

[0088] Here, it is assumed that the combination of the first information and the second information is accepted in the case where the COL-dimensional vector $GV^{\rightarrow}$ belongs to a vector space span<MT_{TFV}> spanned by the row vectors $mt_{\lambda}^{\rightarrow}$ of the submatrix MT_{TFV} described above and that the combination of the first information and the second information is rejected in the case where the COL-dimensional vector $GV^{\rightarrow}$ does not belong thereto. As a result, the access structure described above is realized. Note that, in the case where the labeled matrix LMT (MT, LAB) corresponds to the first information, the case where the access structure accepts the combination of the first information and the second infor-

mation is expressed by "the access structure accepts the second information", and the case where the access structure does not accept the combination of the first information and the second information is expressed by "the access structure rejects the second information".

$$\text{Accepted if } GV^{\rightarrow} \in \text{span}\langle MT_{TFV}\rangle$$

$$\text{Rejected if } \neg(GV^{\rightarrow} \in \text{span}\langle MT_{TFV}\rangle)$$

Further, in the case where $GV^{\rightarrow} \in \text{span}\langle MT_{TFV}\rangle$, a coefficient const($\mu$) that satisfies the following expression exists.

$$SE = \Sigma_{\mu \in SET} const(\mu) \cdot share(\mu) \qquad \ldots (45)$$

$$\{const(\mu) \in F_q \mid \mu \in SET\}, SET \subseteq \{1, \ldots, \lambda \mid LIT(\lambda) = 1\}$$

The coefficient const(μ) can be obtained by the polynomial time of the size of the matrix MT.

<Basic Configuration of Function Cryptosystem using Access Structure>

[0089] Description will be given below of a basic configuration when key encapsulation mechanisms (KEM) are configured according to a function cryptosystem using the access structure. This configuration includes: Setup (1^{sec}, (Ψ; n (1), ..., n(Ψ))); GenKey (PK, MSK, LMT (MT, LAB)); Enc (PK, M, {λ, $v(\lambda)^{\rightarrow}$ |λ = 1, ..., Ψ}) ($v_1(\lambda) = 1_F$); and Dec (PK, SKS, C). Further, the first element $W_1(\lambda)$ of the second information VSET2 = {λ, $w(\lambda)^{\rightarrow}$ |λ = 1, ..., Ψ} is defined as 1_F.

[0090] [Setup (1^{sec}, (Ψ; n(1), ..., n(Ψ))): setup]

- Input: 1^{sec}, (Ψ; n(1), ..., n(Ψ))
- Output: master key information MSK, public parameter PK

In the setup, the following process is executed for each ψ = 0, ..., Ψ.
(Setup-1) With 1^{sec} being received as an input, the order q, the elliptic curve E, the cyclic groups G_1, G_2, and G_T, and the bilinear map e_ψ (ψ = 0, ..., Ψ) at the security parameter sec are generated (param = (q, E, G_1, G_2, G_T, e_ψ)).
(Setup-2) $\tau' \in F_q$ is selected, and matrixes $X(\psi)$, $X^*(\psi)$ that satisfy $X^*(\psi) = \tau' \cdot (X(\psi)^{-1})^T$ are selected.
(Setup-3) Coordinate conversion is applied to the basis vector $a_i(\psi)$ (i = 1, ..., n(ψ) + $\zeta(\psi)$) according to Expression (21), and the (n(ψ) + $\zeta(\psi)$)-dimensional basis vector $b_i(\psi)$ (i = 1, ..., n(ψ) + $\zeta(\psi)$) is generated. The (n(ψ) + $\zeta(\psi)$) row by (n(ψ) + $\zeta(\psi)$) column matrix B(ψ) having the basis vector $b_i(\psi)$ (i = 1, ..., n(ψ) + (ψ)) as elements is generated.
(Setup-4) Coordinate conversion is applied to the basis vector $a_i^*(\psi)$ (i = 1, ..., n(ψ) + $\zeta(\psi)$) according to Expression (23), and the (n(ψ) + $\zeta(\psi)$)-dimensional basis vector $b_i^*(\psi)$ (i = 1, ..., n(ψ) + $\zeta(\psi)$) is generated. The (n(ψ) + $\zeta(\psi)$) row by (n(ψ) + $\zeta(\psi)$) column matrix B*(ψ) having the basis vector $b_i^*(\psi)$ (i = 1, ..., n(ψ) + $\zeta(\psi)$) as elements is generated.
(Setup-5) A set $\{B^*(\psi)^\wedge\}_{\psi=0, \ldots, \Psi}$ of B*(ψ)^ is defined as the master key information MSK = $\{B^*(\psi)^\wedge\}_{\psi=0, \ldots, \Psi}$. Further, a set $\{B(\psi)^\wedge\}_{\psi=0, \ldots, \Psi}$ of B(ψ)^, 1^{sec}, and param are defined as the public parameter PK. Note that B*(ψ)^ is the matrix B*(ψ) or a submatrix thereof, and B(ψ)^ is the matrix B(ψ) or a submatrix thereof. Further, the set $\{B^*(\psi)^\wedge\}_{\psi=0, \ldots, \Psi}$ includes at least $b_1^*(0)$, $b_1^*(\lambda)$, ..., $b_{n(\lambda)}^*(\lambda)$ (λ = 1, ..., Ψ). Further, the set $\{B(\psi)^\wedge\}_{\psi=0, \ldots, \Psi}$ includes at least $b_1(0)$, $b_1(\lambda)$, ..., $b_{n(\lambda)}(\lambda)$ (λ = 1, ..., Ψ). Examples thereof are given below.

$$\cdot\, n(0) + \zeta(0) \geq 5, \zeta(\lambda) = 3 \cdot n(\lambda)$$

$$\cdot\, B(0)^\wedge = (b_1(0)\ b_3(0)\ b_5(0))^T$$

$$\cdot\, B(\lambda)^\wedge = (b_1(\lambda) \ldots b_{n(\lambda)}(\lambda)\ b_{3 \cdot n(\lambda)+1}(\lambda) \ldots b_{4 \cdot n(\lambda)}(\lambda))^T\ (\lambda = 1, \ldots, \Psi)$$

$$\cdot B^*(0)\hat{} = (b_1^*(0)\ b_3^*(0)\ b_4^*(0))^T$$

$$\cdot B^*(\lambda)\hat{} = (b_1^*(\lambda) \ldots b_{n(\lambda)}^*(\lambda)\ b_{2\cdot n(\lambda)+1}^*(\lambda) \ldots b_{3\cdot n(\lambda)}^*(\lambda))^T\ (\lambda = 1, \ldots, \Psi)$$

[0091] [GenKey (PK, MSK, LMT (MT, LAB)): key information generation]

- Input: public parameter PK, master key information MSK, labeled matrix LMT (MT, LAB) corresponding to first information VSET1 = {λ, $v(\lambda)\rightarrow$ I λ = 1, ..., Ψ}
- Output: key information SKS

(GenKey-1) The following process is executed for the secret information SE that satisfies Expressions (35) to (39).

$$D^*(0) = -SE \cdot b_1^*(0) + \Sigma_{\iota=2}^{I} coef_\iota(0) \cdot b_\iota^*(0) \qquad \ldots (46)$$

Note that I is a constant equal to or more than 2 and equal to or less than n(0) + ζ(0). $coif_\tau(0) \in F_q$ is a constant or a random number. The "random number" means a true random number and a pseudorandom number. An example of D*(0) is given below. Note that $coef_4(0)$ in Expression (47) is a random number.

$$D^*(0) = -SE \cdot b_1^*(0) + b_3^*(0) + coef_4(0) \cdot b_4^*(0) \qquad \ldots (47)$$

(GenKey-2) The following process is executed for share(λ) (λ = 1, ..., Ψ) that satisfies Expressions (35) to (39).
The following expression is generated for λ that satisfies LAB(λ) = $v(\lambda)\rightarrow$.

$$D^*(\lambda) = (share(\lambda) + coef(\lambda) \cdot v_1(\lambda)) \cdot b_1^*(\lambda) + \Sigma_{\iota=2}^{n(\lambda)} coef(\lambda) \cdot v_\iota(\lambda) \cdot b_\iota^*(\lambda)$$

$$+ \Sigma_{\iota=n(\lambda)+1}^{n(\lambda)+\zeta(\lambda)} coef_\iota(\lambda) \cdot b_\iota^*(\lambda) \qquad \ldots (48)$$

The following expression is generated for λ that satisfies LAB(λ) = $\neg v(\lambda)\rightarrow$.

$$D^*(\lambda) = share(\lambda) \cdot \Sigma_{\iota=1}^{n(\lambda)} v_\iota(\lambda) \cdot b_\iota^*(\lambda) + \Sigma_{\iota=n(\lambda)+1}^{n(\lambda)+\zeta(\lambda)} coef_\iota(\lambda) \cdot b_\iota^*(\lambda) \qquad \ldots (49)$$

Note that coef(λ), $coef_\tau(\lambda) \in F_q$ are a constant or a random number. An example thereof is given below.
The following expression is generated for λ that satisfies LAB(λ) = $v(\lambda)\rightarrow$.

$$D^*(\lambda) = (share(\lambda) + coef(\lambda) \cdot v_1(\lambda)) \cdot b_1^*(\lambda) + \Sigma_{\iota=2}^{n(\lambda)} coef(\lambda) \cdot v_\iota(\lambda) \cdot b_\iota^*(\lambda) + \Sigma_{\iota=2\cdot n(\lambda)+1}^{3\cdot n(\lambda)} coef_\iota(\lambda) \cdot b_\iota^*(\lambda) \qquad \ldots (50)$$

The following expression is generated for λ that satisfies $LAB(\lambda) = \neg v(\lambda)^{\rightarrow}$.

$$D^{*}(\lambda) = share(\lambda) \cdot \Sigma_{\iota=1}^{n(\lambda)} v_{\iota}(\lambda) \cdot b_{\iota}^{*}(\lambda) + \Sigma_{\iota=2\cdot n(\lambda)+1}^{3\cdot n(\lambda)} coef_{\iota}(\lambda) \cdot b_{\iota}^{*}(\lambda) \quad \ldots (51)$$

Note that $coef(\lambda)$ and $coef_{\tau}(\lambda)$ in Expressions (50) and (51) are a random number.

(GenKey-3) Key information

The following expression is generated.

$$SKS = (LMT(MT, LAB), D^{*}(0), D^{*}(1), \ldots, D(\Psi)) \quad \ldots (52)$$

[0092] [Enc (PK, M, VSET2): encryption]

- Input: public parameter PK, plaintext M, second information $VSET2 = \{\lambda, w(\lambda)^{\rightarrow} \mid \lambda = 1, \ldots, \Psi\}$ $(w_1(\lambda) = 1_F)$
- Output: ciphertext C

(Enc-1) Through the following process, the ciphertext $C(\psi)$ $(\psi = 0, \ldots, \Psi)$ of the common key K is generated.

$$C(0) = \upsilon \cdot b_1(0) + \Sigma_{\iota=2}^{I} \upsilon_{\iota}(0) \cdot b_{\iota}(0) \quad \ldots (53)$$

$$C(\lambda) = \upsilon \cdot \Sigma_{\iota=1}^{n(\lambda)} w_{\iota}(\lambda) \cdot b_{\iota}(\lambda) + \Sigma_{\iota=n(\lambda)+1}^{n(\lambda)+\zeta(\lambda)} \upsilon_{\iota}(\lambda) \cdot b_{\iota}(\lambda) \quad \ldots (54)$$

Note that u, $\upsilon_{\tau}(\psi) \in F_q$ $(\psi = 0, \ldots, \Psi)$ are a constant or a random number, and satisfy the following expressions.

$$(coef_2(0), \ldots, coef_I(0)) \cdot (\upsilon_2(0), \ldots, \upsilon_I(0)) = \upsilon' \quad \ldots (55)$$

$$coef_{\iota}(\lambda) \cdot \upsilon_{\iota}(\lambda) = 0_F \ (\iota = n(\lambda) + 1, \ldots, n(\lambda) + \zeta(\lambda)) \quad \ldots (56)$$

u' is, for example, any one of $\upsilon_2(0), \ldots, \upsilon_I(0)$. For example, $\upsilon, \upsilon_3(0), \upsilon_5(0), \upsilon_{3\cdot n(\lambda)+1}(\lambda), \ldots, \upsilon_{4\cdot n(\lambda)}(\lambda)$ are a random number, $\zeta(\lambda) = 3 \cdot n(\lambda)$, and I = 5. Further, the following expressions are satisfied.

$$(\upsilon_2(0), \ldots, \upsilon_I(0)) = (0_F, \upsilon_3(0), 0_F, \upsilon_5(0))$$

$$\upsilon' = \upsilon_3(0)$$

$$(\upsilon_{n(\lambda)+1}(\lambda), \ldots, \upsilon_{3\cdot n(\lambda)}(\lambda)) = (0_F, \ldots, 0_F)$$

(Enc-2) Common key

The following expression is generated.

$$K = g_T^{\tau\cdot\tau'\cdot\upsilon'} \in G_T \quad \ldots (57)$$

For example, in the case where $\tau = \tau' = 1_F$, the following expression is satisfied.

$$K = g_T^{\upsilon'} \in G_T \qquad \ldots (58)$$

(Enc-3) With the use of the common key K, the following ciphertext of the plaintext M is generated.

$$C(\Psi + 1) = Enc_K(M) \qquad \ldots (59)$$

Note that a common key cryptosystem Enc may be, for example, Camellia (registered trademark) that is configured so as to be encryptable using the common key K, AES, and the exclusive OR of the common key and the plaintext. For another simple example, $Enc_K(M)$ may be generated in the following manner.

$$C(\Psi + 1) = g_T^{\upsilon'} \cdot M \qquad \ldots (60)$$

where $M \in G_T$.
(Enc-4) Ciphertext
The following expression is generated.

$$C = (VSET2, C(0), \{C(\lambda)\}_{(\lambda,\, w(\lambda)\rightarrow)\in VSET2}, C(\Psi + 1)) \qquad \ldots(61)$$

Note that the subscript "$w(\lambda)^{\rightarrow}$" represents "$w(\lambda)^{\rightarrow}$".
[0093] [Dec (PK, SKS, C): decryption]

- Input: public parameter PK, key information SKS, ciphertext C
- Output: plaintext M'

(Dec-1) For $\lambda = 1, \ldots, \Psi$, it is determined whether or not the inner product $v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow}$ of the $n(\lambda)$-dimensional vector $v(\lambda)^{\rightarrow}$ and the $n(\lambda)$-dimensional vector $w(\lambda)^{\rightarrow}$ is 0, the $n(\lambda)$-dimensional vector $v(\lambda)^{\rightarrow}$ being each label $LAB(\lambda)$ of the labeled matrix LMT (MT, LAB) included in the key information SKS, the $n(\lambda)$-dimensional vector $w(\lambda)^{\rightarrow}$ being included in VSET2 of the ciphertext C. Then, whether or not $GV^{\rightarrow} \in span<MT_{TFV}>$ is determined by the result of this determination. If $GV^{\rightarrow} \notin span<MT_{TFV}>$, the ciphertext C is rejected. If $GV^{\rightarrow} \in span<MT_{TFV}>$, the ciphertext C is accepted.
(Dec-2) If the ciphertext C is accepted, $SET \subseteq \{ 1, \ldots, \lambda, \mid LIT(\lambda) = 1 \}$ and the coefficient $const(\mu)$ ($\mu \in SET$) that satisfies Expression (45) are calculated.
(Dec-3) Common key
The following expression is generated.

$$K = e_0(C(0), D^*(0)) \cdot \prod_{\mu \in SET \wedge LAB(\mu) = v(\mu)^{\rightarrow}} e_\mu(C(\mu), D^*(\mu))^{const(\mu)} \cdot \prod_{\mu \in SET \wedge LAB(\mu) = \neg v(\mu)^{\rightarrow}} e_\mu(C(\mu), D^*(\mu))^{const(\mu)/(v(\mu)^{\rightarrow} \cdot w(\mu)^{\rightarrow})} \qquad \cdots (62)$$

Here, the following expression is satisfied on the basis of Expressions (6), (25), and (55).

$$
\begin{aligned}
& e_0(C(0), D^*(0)) \\
& = e_0(\upsilon \cdot b_1(0) + \textstyle\sum_{\iota=2}^{I} \upsilon_\iota(0) \cdot b_\iota(0), -SE \cdot b_1^*(0) + \textstyle\sum_{\iota=2}^{I} coef_\iota(0) \cdot b_\iota^*(0)) \\
& = e_0(\upsilon \cdot b_1(0), -SE \cdot b_1^*(0)) \cdot \textstyle\prod_{\iota=2}^{I} e_0(\upsilon_\iota(0) \cdot b_\iota(0), coef_\iota(0) \cdot b_\iota^*(0))) \\
& = e_0(b_1(0), b_1^*(0))^{-SE \cdot \upsilon} \cdot \textstyle\prod_{\iota=2}^{I} e_0(b_\iota(0), b_\iota^*(0))^{\upsilon_\iota(0) \cdot coef_\iota(0)}) \\
& = g_T^{\tau \cdot \tau' \cdot \delta(1,1) \cdot (-SE \cdot \upsilon)} \cdot \textstyle\prod_{\iota=2}^{I} g_T^{\tau \cdot \tau' \cdot \delta(\iota,\iota) \cdot \upsilon_\iota(0) \cdot coef_\iota(0)} \\
& = g_T^{\tau \cdot \tau' \cdot (-SE \cdot \upsilon + \upsilon')}
\end{aligned}
\qquad \cdots (63)
$$

Further, the following expression is satisfied on the basis of Expressions (6), (25), (41), (48), (54), and (56) and $w_1(\lambda) = 1_F$.

$$
\begin{aligned}
& \prod_{\mu \in SET \wedge LAB(\mu) = \nu(\mu)^{\rightarrow}} e_\mu(C(\mu), D^*(\mu))^{const(\mu)} \\
& = \prod_{\mu \in SET \wedge LAB(\mu) = \nu(\mu)^{\rightarrow}} e_\mu(\upsilon \cdot \textstyle\sum_{\iota=1}^{n(\mu)} w_\iota(\mu) \cdot b_\iota(\mu) + \textstyle\sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)} \upsilon_\iota(\mu) \cdot b_\iota(\mu), \\
& share(\mu) \cdot b_1^*(\mu) + \textstyle\sum_{\iota=1}^{n(\mu)} coef(\mu) \cdot v_\iota(\mu) \cdot b_\iota^*(\mu) \\
& + \textstyle\sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)} coef_\iota(\mu) \cdot b_\iota^*(\mu))^{const(\mu)} \\
& = \prod_{\mu \in SET \wedge LAB(\mu) = \nu(\mu)^{\rightarrow}} \left\{ \begin{array}{l} e_\mu(\upsilon \cdot \textstyle\sum_{\iota=1}^{n(\mu)} w_\iota(\mu) \cdot b_\iota(\mu), share(\mu) \cdot b_1^*(\mu)) \\ \cdot e_\mu(\upsilon \cdot \textstyle\sum_{\iota=1}^{n(\mu)} w_\iota(\mu) \cdot b_\iota(\mu), \textstyle\sum_{\iota=1}^{n(\mu)} coef(\mu) \cdot v_\iota(\mu) \cdot b_\iota^*(\mu)) \end{array} \right\}^{const(\mu)} \\
& = \prod_{\mu \in SET \wedge LAB(\mu) = \nu(\mu)^{\rightarrow}} \left(g_T^{\tau \cdot \tau' \cdot \upsilon \cdot share(\mu)} \cdot \textstyle\prod_{\iota=1}^{n(\mu)} g_T^{\tau \cdot \tau' \cdot \upsilon \cdot coef(\mu) \cdot w_\iota(\mu) \cdot v_\iota(\mu)} \right)^{const(\mu)} \\
& = \prod_{\mu \in SET \wedge LAB(\mu) = \nu(\mu)^{\rightarrow}} g_T^{\tau \cdot \tau' \cdot \upsilon \cdot const(\mu) \cdot share(\mu)}
\end{aligned}
\qquad \cdots (64)
$$

Further, the following expression is satisfied on the basis of Expressions (6), (25), (42), (49), (54), and (56).

$$\prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} e_\mu(C(\mu),D^*(\mu))^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} e_\mu(\upsilon\cdot\sum_{\iota=1}^{n(\mu)} w_\iota(\mu)\cdot b_\iota(\mu)+\sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)}\upsilon_\iota(\mu)\cdot b_\iota(\mu),$$

$$share(\mu)\cdot\sum_{\iota=1}^{n(\mu)} v_\iota(\mu)\cdot b_\iota{}^*(\mu)+\sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)} coef_\iota(\mu)\cdot b_\iota{}^*(\mu))^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} \left\{\prod_{\iota=1}^{n(\mu)} e_\mu\left(b_\iota(\mu),b_\iota{}^*(\mu)\right)^{\upsilon\cdot share(\mu)\cdot w_\iota(\mu)\cdot v_\iota(\mu)}\right\}^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} \left\{\prod_{\iota=1}^{n(\mu)} g_T{}^{\tau\cdot\tau'\cdot\upsilon\cdot share(\mu)\cdot w_\iota(\mu)\cdot v_\iota(\mu)}\right\}^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} \left\{g_T{}^{\tau\cdot\tau'\cdot\upsilon\cdot share(\mu)\cdot v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow}}\right\}^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} g_T{}^{\tau\cdot\tau'\cdot\upsilon\cdot const(\mu)\cdot share(\mu)} \quad \cdots (65)$$

Accordingly, the following expression is satisfied on the basis of Expressions (45) and (63) to (65).

$$K = g_T{}^{\tau\cdot\tau'\cdot(-SE\cdot\upsilon+\upsilon')}\cdot\prod_{\mu\in SET\wedge LAB(\mu)=v(\mu)^{\rightarrow}} g_T{}^{\tau\cdot\tau'\cdot\upsilon\cdot const(\mu)\cdot share(\mu)}$$

$$\cdot\prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} g_T{}^{\tau\cdot\tau'\cdot\upsilon\cdot const(\mu)\cdot share(\mu)}$$

$$= g_T{}^{\tau\cdot\tau'\cdot(-SE\cdot\upsilon+\upsilon')}\cdot g_T{}^{\tau\cdot\tau'\cdot\upsilon\cdot SE} = g_T{}^{\tau\cdot\tau'\cdot\upsilon'} \quad \cdots (66)$$

For example, in the case where $\tau = \tau' = 1_F$, the following expression is satisfied.

$$K = g_T{}^{\upsilon'} \in G_T \quad \ldots (67)$$

(Dec-4) With the use of the common key K, the following plaintext is generated.

$$M' = Dec_K(C(\Psi+1)) = Dec_K(C(\Psi+1)) \quad \ldots (68)$$

For example, in the case of the common key cryptosystem shown in Expression (60), the plaintext M' is generated by the following expression.

$$M' = C(\Psi+1)/K \quad \ldots (69)$$

[0094] Note that $g_T{}^{\tau}$, $g_T{}^{\tau'}$, and $g_T{}^{\tau\cdot\tau'}$ may be treated as generating elements of G_T instead of treating g_T as a generating

element of G_T. Further, a combination of $C(\lambda)$ and $D^*(\lambda)$ may be identified using a map that identifies a correspondence relationship between λ of the key information SKS and λ of the ciphertext, and the process of [Dec (PK, SKS, C): decryption] may be executed. Further, 1_F may be set to not only the first element $W_1(\lambda)$ of the second information VSET2 = $\{\lambda, w(\lambda)\rightarrow | \lambda = 1, ..., \Psi\}$ but also the $n(\lambda)$-th element $v_{n(\lambda)}(\lambda)$ of the first information VSET1 = $\{\lambda, v(\lambda)\rightarrow | \lambda = 1, ..., \Psi\}$. Further, in the case where the element $W_1(\lambda)$ is not 1_F, $w(\lambda)\rightarrow$ / $w_1(\lambda)$ may be used instead of $w(\lambda)\rightarrow$. In the case where the element $v_{n(\lambda)}(\lambda)$ is not 1_F, $v(\lambda)\rightarrow$ / $v_{n(\lambda)}(\lambda)$ may be used instead of $v(\lambda)\rightarrow$. Further, the second information VSET2 = $\{\lambda, w(\lambda)\rightarrow|\lambda, = 1, ..., \Psi\}$ may be used instead of the first information VSET1 = $\{\lambda, v(\lambda)\rightarrow | \lambda = 1, ..., \Psi\}$, and the first information VSET1 = $\{\lambda, v(\lambda)\rightarrow | \lambda = 1, ..., \Psi\}$ may be used instead of the second information VSET2 = $\{\lambda, w(\lambda)\rightarrow | \lambda = 1, ..., \Psi\}$. In this case, 1_F is set to the first element $v_1(\lambda)$ of the first information VSET1 = $\{\lambda, v(\lambda)\rightarrow | \lambda = 1, ..., \Psi\}$.

[0095] Next, predicate encryption using inner products will be described as an example of the predicate encryption that is one mode of the functional encryption. Expression numbers are newly assigned below. It should be noted that the same wording and symbols as those used in the above descriptions may have different meanings in the following description for the sake of explanation. The predicate encryption corresponds to functional encryption using a 1-out-of-1 sharing scheme.

[Definitions]

[0096] Matrix: A rectangular arrangement of elements of a set in which a calculation is defined. Not only elements of a ring but also elements of a group can form a matrix.

$(\cdot)^T$: Transposed matrix of $\cdot$

$(\cdot)^{-1}$: Inverse matrix of $\cdot$

^: Logical AND

v: Logical OR

Z: Set of integers

k: Security parameter ($k \in Z$, $k > 0$)

{0, 1}*: Binary sequence having a desired bit length. An example is a sequence formed of integers 0 and 1. However, {0, 1} * is not limited to sequences formed of integers 0 and 1. {0, 1}* is a finite field of order 2 or its extended field.

$\{0, 1\}^\zeta$: Binary sequence having a bit length ζ ($\zeta \in Z$, $\zeta > 0$). An example is a sequence formed of integers 0 and 1. However, $\{0, 1\}^\zeta$ is not limited to sequences formed of integers 0 and 1. $\{0, 1\}^\zeta$ is a finite field of order 2 (when $\zeta = 1$) or its extended field (when $\zeta > 1$).

(+): Exclusive OR operator between binary sequences. For example, the following is satisfied: 10110011 (+) 11100001 = 01010010.

[0097] F_q: Finite field of order q, where q is an integer equal to or larger than 1. For example, the order q is a prime number of a power of a prime number. In other words, the finite field F_q is a prime field or an extended field of the prime field, for example. When the finite field F_q is a prime field, remainder calculations to modulus q can be easily performed, for example. When the finite field F_q is an extended field, remainder calculations modulo an irreducible polynomial can be easily performed, for example. A specific method for configuring a finite field Fq is disclosed, for example, in reference literature 1, "ISO/IEC 18033-2: Information technology--Security techniques--Encryption algorithms--Part 2: Asymmetric ciphers".

[0098] 0_F: Additive unit element of the finite field F_q

1_F: Multiplicative unit element of the finite field F_q

$\delta(i, j)$: Kronecker's delta function. When $i = j$, $\delta(i, j) = 1_F$. When $i \neq j$, $\delta(i, j) = 0_F$.

[0099] E: Elliptic curve defined on the finite field F_q. It is defined as a special point O called the point of infinity plus a set of points (x, y) satisfying $x, y \in F_q$ and the Weierstrass equation in an affine coordinate system

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in F_q$. A binary operation + called an elliptic addition can be defined for any two points on the elliptic curve E, and a unary operation - called an elliptic inverse can be defined for any one point on the elliptic curve E. It is well known that a finite set of rational points on the elliptic curve E forms a group with respect to the elliptic addition. It is also well known that an operation called an elliptic scalar multiplication can be defined with the elliptic addition. A specific operation method of elliptic operations such as the elliptic addition on a computer is also well known. (For example, see reference literature 2, "RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", and reference literature 3, Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, "Elliptic Curves in Cryptography", Pearson Education, ISBN 4-89471-431-0.)

A finite set of rational points on the elliptic curve E has a subgroup of order p ($p \geq 1$). When the number of elements in

a finite set of rational points on the elliptic curve E is #E and p is a large prime number that can divide #E without a remainder, for example, a finite set E[p] of p equally divided points on the elliptic curve E forms a subgroup of a finite set of rational points on the elliptic curve E. The p equally divided points on the elliptic curve E are points A on the elliptic curve E which satisfy the elliptic scalar multiplication pA = O.

[0100] G_1, G_2, G_T: Cyclic groups of order q. Examples of the cyclic groups G_1 and G_2 include the finite set E[p] of p equally divided points on the elliptic curve E and subgroups thereof. G_1 may equal G_2, or G_1 may not equal G_2. Examples of the cyclic group G_T include a finite set constituting an extended field of the finite field F_q. A specific example thereof is a finite set of the p-th root of 1 in the algebraic closure of the finite field F_q.

[0101] Operations defined on the cyclic groups G_1 and G_2 are expressed as additions, and an operation defined on the cyclic group G_T is expressed as a multiplication. More specifically, $\chi \cdot \Omega \in G_1$ for $\chi \in F_q$ and $\Omega \in G_1$ means that the operation defined in the cyclic group G_1 is applied to $\Omega \in G_1$ χ times, and $\Omega_1 + \Omega_2 \in G_1$ for $\Omega_1, \Omega_2 \in G_1$ means that the operation defined in the cyclic group G_1 is applied to $\Omega_1 \in G_1$ and $\Omega_2 \in G_1$. In the same way, $\chi \cdot \Omega \in G_2$ for $\chi \in F_q$ and $\Omega \in G_2$ means that the operation defined in the cyclic group G_2 is applied to $\Omega \in G_2$ χ times, and $\Omega_1 + \Omega_2 \in G_2$ for Ω_1, $\Omega_2 \in G_2$ means that the operation defined in the cyclic group G_2 is applied to $\Omega_1 \in G_2$ and $\Omega_2 \in G_2$. In contrast, $\Omega^{\chi} \in G_T$ for $\chi \in F_q$ and $\Omega \in G_T$ means that the operation defined in the cyclic group G_T is applied to $\Omega \in G_T$ χ times, and $\Omega_1 \cdot \Omega_2 \in G_T$ for $\Omega_1, \Omega_2 \in G_T$ means that the operation defined in the cyclic group G_T is applied to $\Omega_1 \in G_T$ and $\Omega_2 \in G_T$.

[0102] G_1^{n+1}: Direct product of (n + 1) cyclic groups G_1 ($n \geq 1$)
G_2^{n+1}: Direct product of (n + 1) cyclic groups G_2
g_1, g_2, g_T: Generating elements of the cyclic groups G_1, G_2, G_T
V: (n + 1)-dimensional vector space formed of the direct product of the (n + 1) cyclic groups G_1
V*: (n + 1)-dimensional vector space formed of the direct product of the (n + 1) cyclic groups G_2

[0103] e: Function (bilinear function) for calculating a non-degenerate bilinear map that maps the direct product $G_1^{n+1} \times G_2^{n+1}$ of the direct product G_1^{n+1} and the direct product G_2^{n+1} to the cyclic group G_T. The bilinear function e receives (n + 1) elements γ_L (L = 1, ..., n + 1) ($n \geq 1$) of the cyclic group G_1 and (n + 1) elements γ_L^* (L = 1, ..., n + 1) of the cyclic group G_2 and outputs one element of the cyclic group G_T.

$$e: \quad G_1^{n+1} \times G_2^{n+1} \rightarrow G_T \qquad (2)$$

[0104] The bilinear function e satisfies the following characteristics:

- Bilinearity: The following relationship is satisfied for all $\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$, and v, $\kappa \in F_q$

$$e(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e(\Gamma_1, \Gamma_2)^{\nu \cdot \kappa} \qquad (3)$$

- Non-degeneracy: This function does not map all

$$\Gamma_1 \in G_1^{n+1}, \Gamma_2 \in G_2^{n+1} \qquad (4)$$

  onto the unit element of the cyclic group G_T.
- Computability: There exists an algorithm for efficiently calculating $e(\Gamma_1, \Gamma_2)$ for all $\Gamma_1 \in G_1^{n+1}$, $F_2 \in G_2^{n+1}$.

[0105] The following function for calculating a non-degenerate bilinear map that maps the direct product $G_1 \times G_2$ of the cyclic group G_1 and the cyclic group G_2 to the cyclic group G_T constitutes the bilinear function e.

$$\text{Pair}: \quad G_1 \times G_2 \rightarrow G_T \qquad (5)$$

The bilinear function e receives an (n + 1)-dimensional vector (γ_1, ..., γ_{n+1}) formed of (n + 1) elements γ_L (L = 1, ..., n + 1) of the cyclic group G_1 and an (n + 1)-dimensional vector (γ_1^*, ..., γ_{n+1}^*) formed of (n + 1) elements γ_L^* (L = 1, ..., n + 1) of the cyclic group G_2 and outputs one element of the cyclic group G_T.

$$e = \prod_{L=1}^{n+1} \text{Pair}(\gamma_L, \gamma_L^*) \qquad (6)$$

The bilinear function Pair receives one element of the cyclic group G_1 and one element of the cyclic group G_2 and outputs one element of the cyclic group G_T, and satisfies the following characteristics:

- Bilinearity: The following relationship is satisfied for all $\Omega_1 \in G_1$, $\Omega_2 \in G_2$, and $\nu, \kappa \in F_q$

$$\mathrm{Pair}(\nu\cdot\Omega_1, \kappa\cdot\Omega_2) = \mathrm{Pair}(\Omega_1, \Omega_2)^{\nu\cdot\kappa} \qquad (7)$$

- Non-degeneracy: This function does not map all

$$\Omega_1 \in G_1, \Omega_2 \in G_2 \qquad (8)$$

onto the unit element of the cyclic group G_T.

- Computability: There exists an algorithm for efficiently calculating $\mathrm{Pair}(\Omega_1, \Omega_2)$ for all $\Omega_1 \in G_1$, $\Omega_2 \in G_2$.

[0106] A specific example of the bilinear function Pair is a function for performing a pairing operation such as Weil pairing or Tate pairing. (See reference literature 4, Alfred. J. Menezes, "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, ISBN 0-7923-9368-6, pp. 61-81, for example.) A modified pairing function $e(\Omega_1, \mathrm{phi}(\Omega_2))$ ($\Omega_1 \in G_1$, $\Omega_2 \in G_2$) obtained by combining a function for performing a pairing operation, such as Tate pairing, and a predetermined function phi according to the type of the elliptic curve E may be used as the bilinear function Pair (see reference literature 2, for example). As the algorithm for performing a pairing operation on a computer, the Miller algorithm (see reference literature 5, V. S. Miller, "Short Programs for Functions on Curves", 1986, http://crypto.stanford.edu/miller/miller.pdf) or some other known algorithm can be used. Methods for configuring a cyclic group and an elliptic curve used to efficiently perform a pairing operation have been known. (For example, see reference literature 2, described earlier, reference literature 6, A. Miyaji, M. Nakabayashi, and S. Takano, "New Explicit Conditions of Elliptic Curve Traces for FR Reduction", IEICE Trans. Fundamentals, Vol. E84-A, No. 5, pp. 1234-1243, May 2001, reference literature 7, P. S. L. M. Barreto, B. Lynn, M. Scott, "Constructing Elliptic Curves with Prescribed Embedding Degrees", Proc. SCN '2002, LNCS 2576, pp. 257-267, Springer-Verlag. 2003, and reference literature 8, R. Dupont, A. Enge, F. Morain, "Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields", http://eprint.iacr.org/2002/094/).

[0107] a_i (i = 1, ..., n + 1): (n + 1)-dimensional basis vector having (n + 1) elements of the cyclic group G_1 as elements. An example of the basis vector a_i is an (n + 1)-dimensional basis vector having $\kappa_1\cdot g_1 \in G_1$ as an i-dimensional element and the unit element (expressed as "0" in additive expression) of the cyclic group G_1 as the remaining n elements. In that case, each element of the (n + I)-dimensional basis vector a_i (i = 1, ..., n + 1) can be listed as follows:

$$\begin{aligned} a_1 &= (\kappa_1\cdot g_1, 0, 0, ..., 0) \\ a_2 &= (0, \kappa_1\cdot g_1, 0, ..., 0) \\ &\cdots\cdots \\ a_{n+1} &= (0, 0, 0, ..., \kappa_1\cdot g_1) \end{aligned} \qquad (9)$$

Here, κ_1 is a constant formed of the elements of the finite field F_q other than the additive unit element 0_F. An example of $\kappa_1 \in F_q$ is $\kappa_1 = 1_F$. The basis vector a_i is an orthogonal basis. Each (n + 1)-dimensional vector having (n + 1) elements of the cyclic group G_1 as elements is expressed by a linear sum of (n + 1)-dimensional basis vectors a_i (i = 1, ..., n + 1). Therefore, the (n + 1)-dimensional basis vectors a_i span the vector space V, described earlier.

[0108] a_i^* (i = 1, ..., n + 1): (n + 1)-dimensional basis vector having (n + 1) elements of the cyclic group G_2 as elements. An example of the basis vector a_i^* is an (n + 1)-dimensional basis vector having $\kappa_2\cdot g_2 \in G_2$ as an i-dimensional element and the unit element (expressed as "0" in additive expression) of the cyclic group G_2 as the remaining n elements. In that case, each element of the (n + I)-dimensional basis vector a_i^* (i = 1, ..., n + 1) can be listed as follows:

$$a_1^* = (\kappa_2 \cdot g_2, 0, 0, ..., 0)$$

$$a_2^* = (0, \kappa_2 \cdot g_2, 0, ..., 0) \qquad (10)$$

$$.....$$

$$a_{n+1}^* = (0, 0, 0, ..., \kappa_2 \cdot g_2)$$

Here, κ_2 is a constant formed of the elements of the finite field F_q other than the additive unit element 0_F. An example of $\kappa_2 \in \kappa_q$ is $\kappa_2 = 1_F$. The basis vector a_i^* is an orthogonal basis. Each (n + 1)-dimensional vector having (n + 1) elements of the cyclic group G_2 as elements is expressed by a linear sum of (n + 1)-dimensional basis vectors a_i^* (i = 1, ..., n + 1). Therefore, the (n + 1)-dimensional basis vectors a_i^* span the vector space V*, described earlier.

[0109] The basis vector a_i and the basis vector a_i^* satisfy the following expression for the elements $\tau = \kappa_1 \cdot \kappa_2$ of the finite field F_q other than 0_F:

$$e(a_i, a_j^*) = g_T^{\tau\delta(i, j)} \qquad (11)$$

When i = j, the following expression is satisfied from Expressions (6) and (7).

$$\begin{aligned} e(a_i, a_j^*) &= Pair(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2) \cdot Pair\ (0, 0) \cdot ... \cdot Pair(0, 0) \\ &= Pair(g_1, g_2)^{\kappa 1 \kappa 2} \cdot Pair\ (g_1, g_2)^{0 \cdot 0} \cdot ... \cdot Pair(g_1, g_2)^{0 \cdot 0} \\ &= Pair(g_1, g_2)^{\kappa 1 \kappa 2} = g_T^{\tau} \end{aligned}$$

When $i \neq j$, $e(a_i, a_j^*)$ does not include $Pair(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2)$ and is the product of Pair $(\kappa_1 \cdot g_1, 0)$, Pair $(0, \kappa_2 \cdot g_2)$, and Pair(0, 0). In addition, the following expression is satisfied from Expression (7).

$$Pair\ (g_1, 0) = Pair\ (0, g_2) = Pair(g_1, g_2)^{0 \cdot 0}$$

Therefore, when $i \neq j$, the following expression is satisfied.

$$e(a_i, a_j^*) = e(g_1, g_2)^0 = g_T^{\ 0}$$

Especially when $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (for example, $\kappa_1 = \kappa_2 = 1_F$), the following expression is satisfied.

$$e(a_i, a_j^*) = g_T^{\delta(i, j)} \qquad (12)$$

Here, $gT^0 = 1$ is the unit element of the cyclic group G_T, and $g_T^1 = g_T$ is a generating element of the cyclic group G_T. In that case, the basis vector a_i and the basis vector a_i^* are a dual normal orthogonal basis, and the vector space V and the vector space V* are a dual vector space that constitute bilinear mapping (dual pairing vector space (DPVS)).

[0110] A: An (n + 1) row by (n + 1) column matrix having the basis vector a_i (i = 1, ..., n + 1) as elements. When the basis vector a_i (i = 1, ..., n + 1) is expressed by Expression (9), for example, the matrix A is as follows:

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} \kappa_1 \cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1 \cdot g_1 \end{pmatrix} \quad \cdots(13)$$

[0111] A*: A (n + 1) row by (n + 1) column matrix having the basis vector a_i^* (i = 1, ..., n + 1) as elements. When the basis vector a_i^* (i = 1, ..., n + 1) is expressed by Expression (10), for example, the matrix A* is as follows:

$$A^* = \begin{pmatrix} a_1^* \\ a_2^* \\ \vdots \\ a_{n+1}^* \end{pmatrix} = \begin{pmatrix} \kappa_2 \cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2 \cdot g_2 \end{pmatrix} \quad \cdots(14)$$

[0112] X: A (n + 1) row by (n + 1) column matrix having elements of the finite field Fq as elements. The matrix X is used to apply coordinate conversion to the basis vector a_i. When the element located at the i-th row and the j-th column in the matrix X, $\chi_{i,j} \in$ Fq, the matrix X is as follows:

$$X = \begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \quad \cdots(15)$$

Here, each element $\chi_{i,j}$ of the matrix X is called a conversion coefficient.

[0113] X*: Transposed matrix of the inverse matrix of the matrix X. $X^* = (X^{-1})^T$. The matrix X* is used to apply coordinate conversion to the basis vector a_i^*. When the element located at the i-th row and the j-th column in the matrix X*, χ_{ij}^*, $\in$ Fq, the matrix X* is as follows:

$$X^* = \begin{pmatrix} \chi_{1,1}^* & \chi_{1,2}^* & \cdots & \chi_{1,n+1}^* \\ \chi_{2,1}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1}^* & \chi_{n+1,2}^* & \cdots & \chi_{n+1,n+1}^* \end{pmatrix} \quad \cdots(16)$$

Here, each element $\chi_{i,j}^*$ of the matrix X* is called a conversion coefficient.

In that case, when an (n + 1) row by (n + 1) column unit matrix is called I, $X \cdot (X^*)^T = I$. In other words, for the unit matrix shown below,

$$I = \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \cdots(17)$$

the following expression is satisfied.

$$\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \cdot \begin{pmatrix} \chi_{1,1}^* & \chi_{2,1}^* & \cdots & \chi_{n+1,1}^* \\ \chi_{1,2}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n+1}^* & \chi_{2,n+1}^* & \cdots & \chi_{n+1,n+1}^* \end{pmatrix} \quad \cdots(18)$$

$$= \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix}$$

Here, (n + 1)-dimensional vectors will be defined below.

$$\vec{\chi_i} = (\chi_{i,1}, \ldots, \chi_{i,n+1}) \quad (19)$$

$$\vec{\chi_j} = (\chi_{j,1}^*, \ldots, \chi_{j,n+1}^*) \quad (20)$$

The inner product of the (n + 1)-dimensional vectors $\chi_i^{\rightarrow}$ and $\chi_j^{\rightarrow *}$ satisfies the following expression from Expression (18).

$$\vec{\chi_i} \cdot \vec{\chi_j}^* = \delta(i, j) \quad (21)$$

[0114] b_i: (n + 1)-dimensional basis vector having (n + 1) elements of the cyclic group G_1 as elements. The basis vector b_i is obtained by applying coordinate conversion to a_i (i = 1, ..., n + 1) by using the matrix X. Specifically, the basis vector b_i is obtained by the following calculation

$$b_i = \sum_{j=1}^{n+1} \chi_{i,j} \cdot a_j \quad (22)$$

When the basis vector a_j (j = 1, ..., n + 1) is expressed by Expression (9), each element of the basis vector b_i is shown below.

$$b_i = (\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{i,2} \cdot \kappa_1 \cdot g_1, \ldots, \chi_{i,n+1} \cdot \kappa_1 \cdot g_1) \quad (23)$$

Each (n + 1)-dimensional vector having (n + 1) elements of the cyclic group G_1 as elements is expressed by a linear sum of (n + 1)-dimensional basis vectors b_i (i = 1, ..., n + 1). Therefore, the (n + 1)-dimensional basis vectors b_i span the vector space V, described earlier.

[0115] b_i^*: (n + 1)-dimensional basis vector having (n + 1) elements of the cyclic group G_2 as elements. The basis vector b_i^* is obtained by applying coordinate conversion to a_i^* (i = 1, ..., n + 1) by using the matrix X*. Specifically, the basis vector b_i^* is obtained by the following calculation

$$b_i^* = \sum_{j=1}^{n+1} \chi_{i,j}^* \cdot a_j^* \qquad (24)$$

When the basis vector a_j (j = 1, ..., n + 1) is expressed by Expression (10), each element of the basis vector b_i^* is shown below.

$$b_i^* = (\chi_{i,1}^* \cdot \kappa_2 \cdot g_2,\ \chi_{i,2} \cdot \kappa_2 \cdot g_2,\ \ldots,\ \chi_{i,n+1}^* \cdot \kappa_2 \cdot g_2) \qquad (25)$$

Each (n + 1)-dimensional vector having (n + 1) elements of the cyclic group G_2 as elements is expressed by a linear sum of (n + 1)-dimensional basis vectors b_i^* (i = 1, ..., n + 1). Therefore, the (n + 1)-dimensional basis vectors b_i^* span the vector space V*, described earlier.

[0116] The basis vector b_i and the basis vector b_i^* satisfy the following expression for the elements $\tau = \kappa_1 \cdot \kappa_2$ of the finite field F_q other than 0_F:

$$e(b_i, b_j^*) = g_T^{\tau\delta(i,j)} \qquad (26)$$

The following expression is satisfied from Expressions (6), (21), (23), and (25).

$$\begin{aligned}
e(b_i, b_j^*) &= \prod_{L=1}^{n+1} \mathrm{Pair}(\chi_{i,L} \cdot \kappa_1 \cdot g_1, \chi_{j,L}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathrm{Pair}(\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{j,1}^* \cdot \kappa_2 \cdot g_2) \cdot \ldots \cdot (\chi_{i,n} \cdot \kappa_1 \cdot g_1, \chi_{j,n}^* \cdot \kappa_2 \cdot g_2) \\
&\quad \times \mathrm{Pair}(\chi_{j,n+1} \cdot \kappa_1 \cdot g_1, \chi_{j,n+1}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,1} \cdot \chi_{j,1}^*} \cdot \ldots \cdot \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,2} \cdot \chi_{j,2}^*} \\
&\quad \times \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+1} \cdot \chi_{j,n+1}^*} \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 (\chi_{i,1} \cdot \chi_{j,1}^* + \chi_{i,2} \cdot \chi_{j,2}^* + \ldots + \chi_{i,n+1} \cdot \chi_{j,n+1}^*)} \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_i^{\rightarrow} \cdot \chi_j^{\rightarrow *}} \\
&= \mathrm{Pair}(g_1, g_2)^{\tau \cdot \delta(i,j)} = g_T^{\tau \cdot \delta(i,j)}
\end{aligned}$$

Especially when $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (for example, $\kappa_1 = \kappa_2 = 1_F$), the following expression is satisfied.

$$e(b_i, b_j^*) = g_T^{\delta(i,j)} \qquad (27)$$

In that case, the basis vector b_i and the basis vector b_i^* are the dual normal orthogonal basis of a dual pairing vector space (the vector space V and the vector space V*).

As long as Expression (26) is satisfied, the basis vectors a_i and a_i^* other than those shown in Expressions (9) and (10) as examples, and the basis vectors b_i and b_i^* other than those shown in Expressions (22) and (24) as examples may

be used.

[0117] B: An (n + 1) row by (n + 1) column matrix having the basis vector b_i (i = 1, ..., n + 1) as elements. B = X·A is satisfied. When the basis vector b_i is expressed by Expression (23), for example, the matrix B is as follows:

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} \chi_{1,1} \cdot \kappa_1 \cdot g_1 & \chi_{1,2} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{1,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{2,1} \cdot \kappa_1 \cdot g_1 & \chi_{2,2} \cdot \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{n+1,1} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{n+1,n} \cdot \kappa_1 \cdot g_1 & \chi_{n+1,n+1} \cdot \kappa_1 \cdot g_1 \end{pmatrix} \quad \cdots (28)$$

[0118] B*: An (n + 1) row by (n + 1) column matrix having the basis vector b_i^* (i = 1, ..., n + 1) as elements. B* = X*·A* is satisfied. When the basis vector b_i^* (i = 1, ..., n + 1) is expressed by Expression (25), for example, the matrix B* is as follows:

$$B^* = \begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_{n+1}^* \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{1,2}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{1,n+1}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{2,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{2,2}^* \cdot \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{n+1,1}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{n+1,n}^* \cdot \kappa_2 \cdot g_2 & \chi_{n+1,n+1}^* \cdot \kappa_2 \cdot g_2 \end{pmatrix} \quad (29)$$

[0119] $\vec{w}$: An n-dimensional vector having elements of the finite field F_q as elements.

$$\vec{w} = (w_1, ..., w_n) \in F_q^n \quad (30)$$

w_μ: The μ-th (μ = 1, ..., n) element of the n-dimensional vector.
$\vec{v}$: An n-dimensional vector having elements of the finite field F_q as elements.

$$\vec{v} = (v_1, ..., v_n) \in F_q^n \quad (31)$$

v_μ: The μ-th (μ = 1, ..., n) element of the n-dimensional vector.

[0120] Collisionless function: A function h that satisfies the following condition with respect to a sufficiently larger security parameter k, or a function regarded as serving as such.

$$\Pr[A(h) = (x, y) | h(x) = h(y) \wedge x \neq y] < \varepsilon(k) \quad (32)$$

Here, Pr[·] is the probability of the event [·]; A(h) is a probability polynomial time algorithm for calculating x and y ($x \neq y$) that satisfy h(x) = h(y) for a function h; and $\varepsilon(k)$ is a polynomial for the security parameter k. An example collisionless function is a hash function such as the cryptographic hash function disclosed in reference literature 1.

[0121] Injective function: A function by which each element belonging to a value range is expressed as the image of only one element in the definition range, or a function regarded as such. An example injection function is a hash function such as the key derivation function (KDF) disclosed in reference literature 1.

[0122] Pseudo-random function: A function belonging to a subset ϕ_ζ when a probability polynomial time algorithm cannot distinguish between the subset ϕ_χ and its whole set Φ_ζ or a function regarded as such. The set Φ_ζ is a set of all functions that map an element of a set $\{0, 1\}^\zeta$ to an element of the set $\{0, 1\}^\zeta$. An example pseudo-random function is a hash function such as that described above.

[0123] H_1: A collisionless function that receives two binary sequences $(\omega_1, \omega_2) \in \{0, 1\}^k \times \{0, 1\}^*$ and outputs two elements $(\psi_1, \psi_2) \in F_q \times F_q$ of the finite field F_q.

$$H_1: \quad \{0, 1\}^k \times \{0, 1\}^* \rightarrow F_q \times F_q \quad (33)$$

An example of the function H_1 is a function that receives the connected bits $\omega_1 \| \omega_2$ of ω_1 and ω_2, performs calculations with a hash function such as the cryptographic hash function disclosed in reference literature 1, a binary-sequence-to-integer conversion function (octet string/integer conversion), and a binary-sequence-to-finite-field-element conversion function (octet string and integer/finite field conversion), and outputs two elements $(\psi_1, \psi_2) \in F_q \times F_q$ of the finite field F_q. It is preferred that the function H_1 be a pseudo-random function.

[0124] H_2: A collisionless function that receives an element of the cyclic group G_T and a binary sequence $(\xi, \omega_2) \in G_T \times \{0, 1\}^*$ and outputs one element $\psi \in F_q$ of the finite field F_q.

$$H_2: \quad G_T \times \{0, 1\}^* \rightarrow F_q \quad (34)$$

An example of the function H_2 is a function that receives an element $\xi \in G_T$ of the cyclic group G_T and a binary sequence $\omega_2 \in \{0, 1\}^*$, inputs the element $\xi \in G_T$ of the cyclic group G_T to the finite-field-element-to-binary-sequence conversion function (octet string and integer/finite field conversion) disclosed in reference literature 1 to obtain a binary sequence, applies a hash function such the cryptographic hash function disclosed in reference literature 1 to the connected bits of the binary sequence and the binary sequence $\omega_2 \in \{0, 1\}^*$, performs a binary-sequence-to-finite-field-element conversion function (octet string and integer/finite field conversion), and outputs one element $\psi \in F_q$ of the finite field F_q. It is preferred from a security viewpoint that the function H_2 be a pseudo-random function.

[0125] R: An injective function that receives an element $\xi \in G_T$ of the cyclic group G_T and outputs one binary sequence $\omega \in \{0, 1\}^k$.

$$R: \quad G_T \rightarrow \{0, 1\}^* \quad (35)$$

An example of the injective function R is a function that receives an element $\xi \in G_T$ of the cyclic group G_T, performs calculations with the finite-field-element-to-binary-sequence conversion function (octet string and integer/finite field conversion) and then with a hash function such as the KDF (key derivation function) disclosed in reference literature 1, and outputs one binary sequence $\omega \in \{0, 1\}^k$. From a security viewpoint, it is preferred that the function R be a collisionless function, and it is more preferred that the function R be a pseudo-random function.

[0126] Enc: A private key encryption function that indicates an encryption process of a private key cryptosystem. Example private key cryptosystems are Camellia(registered trademark) and AES.

$Enc_k(M)$: Ciphertext obtained by encrypting plaintext M by the private key encryption function Enc with the use of a common key K.

Dec: A private key decryption function that indicates a decryption process of the private key cryptosystem.

$Dec_k(C)$: A decryption result obtained by decrypting ciphertext C by the private key decryption function Dec with the use of the common key K.

[Inner product functional encryption]

[0127] The basic configuration of inner product functional encryption will be described below.

<Functional encryption>

[0128] Functional encryption (sometimes called functional encryption) means that ciphertext can be decrypted when a combination of attribute information and logic information makes a predetermined logical expression true. One of the attribute information and logic information is embedded in the ciphertext and the other is embedded in key information. The configuration of conventional functional encryption is, for example, disclosed in reference literature 9, Jonathan Katz, Amit Sahai and Brent Waters, "Function encryption supporting Disjunctions, Polynomial Equations, and Inner Products", one of four papers from Eurocrypt 2008 invited by the Journal of Cryptology.

<Inner product functional encryption>

[0129] Inner product functional encryption means that ciphertext can be decrypted when the inner product of attribute information and logic information handled as vectors is zero. In inner product functional encryption, an inner product of zero is equivalent to a logical expression of true.

[Relationship between logical expression and polynomial]

[0130] In inner product functional encryption, a logical expression formed of a logical OR(s) and/or a logical AND(s) is expressed by a polynomial.
The logical OR $(x = \eta_1) \vee (x = \eta_2)$ of statement 1 indicating that x is η_1 and statement 2 indicating that x is η_2 is expressed by the following polynomial.

$$(x - \eta_1) \cdot (x - \eta_2) \qquad (36)$$

Then, the relationships between true values and the function values of Expression (36) are shown in the following table.

Table 1

Statement 1 $(x = \eta_1)$	Statement 2 $(X=\eta_2)$	Logical OR $(x=\eta_1) \vee (x=\eta_2)$	Function value $(x=\eta_1) \cdot (x=\eta_2)$
True	True	True	0
True	False	True	0
False	True	True	0
False	False	False	Other than 0

[0131] As understood from Table 1, when the logical OR $(x = \eta_1) \vee (x = \eta_2)$ is true, the function value of Expression (36) is zero; and when the logical OR $(x = \eta_1) \vee (x = \eta_2)$ is false, the function value of Expression (36) is a value other than zero. In other words, a logical OR $(x = \eta_1) \vee (x = \eta_2)$ of true is equivalent to a function value of zero in Expression (36). Therefore, the logical OR can be expressed by Expression (36).
[0132] The logical AND $(x = \eta_1) \wedge (x = \eta_2)$ of statement 1 indicating that x is η_1 and statement 2 indicating that x is η_2 is expressed by the following polynomial

$$\iota_1 \cdot (x - \eta_1) + \iota_2 \cdot (x - \eta_2) \qquad (37)$$

where t_1 and t_2 are random numbers. Then, the relationships between true values and the function values of Expression (37) are shown in the following table.

Table 2

Statement 1 ($x = \eta_1$)	Statement 2 ($x = \eta_2$)	Logical AND $(x = \eta_1) \wedge (x = \eta_2)$	Function value $\tau_1 \cdot (x - \eta_1) + \tau_2 \cdot (x - \eta_2)$
True	True	True	0
True	False	False	Other than 0
False	True	False	Other than 0
False	False	False	Other than 0

[0133] As understood from Table 2, when the logical AND $(x = \eta_1) \wedge (x = \eta_2)$ is true, the function value of Expression (37) is zero; and when the logical AND $(x = \eta_1) \wedge (x = \eta_2)$ is false, the function value of Expression (37) is a value other than zero. In other words, a logical AND $(x = \eta_1) \wedge (x = \eta_2)$ of true is equivalent to a function value of zero in Expression (37). Therefore, the logical AND can be expressed by Expression (37).

[0134] As described above, by using Expressions (36) and (37), a logical expression formed of a logical OR(s) and/or a logical AND(s) can be expressed by the polynomial f(x). An example will be shown below.

$$\text{Logical expression:} \quad \{(x = \eta_1) \vee (x = \eta_2) \vee (x = \eta_3)\} \wedge (x = \eta_4) \wedge (x = \eta_5)$$

$$\text{Polynomial:} \quad f(x) = \iota_1 \cdot \{(x - \eta_1) \cdot (x - \eta_2) \cdot (x - \eta_3)\} + \iota_2 \cdot (x - \eta_4) + \iota_3 \cdot (x - \eta_5) \tag{38}$$

In Expression (36), one indeterminate element x is used to express the logical OR. A plurality of indeterminate elements can also be used to express a logical OR. For example, two indeterminate elements x_0 and x_1 are used to express the logical OR $(x_0 = \eta_0) \vee (x_1 = \eta_1)$ of statement 1 indicating that x_0 is η_0 and statement 2 indicating that η_1 is η_1 by the following polynomial.

$$(x_0 - \eta_0) \cdot (x_1 - \eta_1)$$

Three or more indeterminate elements can also be used to express a logical OR by a polynomial.

[0135] In Expression (37), one indeterminate element x is used to express the logical AND. A plurality of indeterminate elements can also be used to express a logical AND. For example, the logical AND $(x_0 = \eta_0) \wedge (x_1 = \eta_1)$ of statement 1 indicating that x_0 is η_0 and statement 2 indicating that x_1 is η_1 can be expressed by the following polynomial.

$$\iota_0 \cdot (x_0 - \eta_0) + \iota_1 \cdot (x_1 - \eta_1)$$

Three or more indeterminate elements can also be used to express a logical AND by a polynomial.

[0136] A logical expression that includes a logical OR(s) and/or a logical AND(s) is expressed with H ($H \geq 1$) types of indeterminate elements $x_0, ..., x_{H-1}$ as the polynomial $f(x_0, ..., x_{H-1})$. It is assumed that a statement for each of the indeterminate elements $x_0, ..., x_{H-1}$ is "x_h is η_h", where η_h ($h = 0, ..., H - 1$) is a constant determined for each statement. Then, in the polynomial $f(x_0, ..., x_{H-1})$ indicating the logical expression, the statement indicating that an indeterminate element x_h is a constant η_h is expressed by the polynomial indicating the difference between the indeterminate element x_h and the constant η_h; each logical OR of statements is expressed by the product of the polynomials indicating the statements; and the logical AND of statements or the logical ORs of statements is expressed by a linear OR of the polynomials indicating the statements or the logical ORs of statements. For example, five indeterminate elements $x_0, ..., x_4$ are used to express a logical expression

$$\{(x_0 = \eta_0) \vee (x_1 = \eta_1) \vee (x_2 = \eta_2)\} \wedge (x_3 = \eta_3) \wedge (x_4 = \eta_4)$$

by the following polynomial

$$f(x0, ..., x4) = \iota_0 \cdot \{(x_0 - \eta_0) \cdot (x_1 - \eta_1) \cdot (x_2 - \eta_2)\} + \iota_1 \cdot (x_3 = \eta_3) + \iota_2 \cdot (x_4 = \eta_4)$$

[Relationship between polynomial and inner product]

[0137] The polynomial $f(x_0, ..., x_{H-1})$ indicating a logical expression can be expressed by the inner product of two n-dimensional vectors. More specifically, a vector having the indeterminate elements of the terms of the polynomial $f(x_0, ..., x_{H-1})$ as elements,

$$\vec{v} = (v_1, ..., v_n)$$

and a vector having the coefficients of the terms of the polynomial $f(x_0, ..., x_{H-1})$ as elements,

$$\vec{w} = (w_1, ..., w_n)$$

are used to generate the inner product thereof,

$$f(x_0, ..., x_{H-1}) = \vec{w} \cdot \vec{v}$$

which is equal to the polynomial $f(x_0, ..., x_{H-1})$. In other words, whether the polynomial $f(x_0, ..., x_{H-1})$ indicating a logical expression is zero is equivalent to whether the inner product of the vector $\vec{v}$ having the indeterminate elements of the terms of the polynomial $f(x_0, ..., x_{H-1})$ as elements and the vector $\vec{w}$ having the coefficients of the terms of the polynomial $f(x_0, ..., x_{H-1})$ as elements is zero.

$$f(x_0, ..., x_{H-1}) = 0 \longleftrightarrow \vec{w} \cdot \vec{v} = 0$$

[0138] For example, a polynomial $f(x) = \theta_0 \cdot x^0 + \theta_1 \cdot x + ... + \theta_{n-1} \cdot x^{n-1}$ can be expressed with two n-dimensional vectors

$$\vec{w} = (w_1, ..., w_n) = (\theta_0, ..., \theta_{n-1}) \quad (39)$$

$$\vec{v} = (v_1, ..., v_n) = (x^0, ..., x^{n-1}) \quad (40)$$

by the inner product thereof.

$$f(x) = \vec{w} \cdot \vec{v} \quad (41)$$

In other words, whether the polynomial f(x) indicating a logical expression is zero is equivalent to whether the inner product in Expression (41) is zero.

$$f(x) = 0 \longleftrightarrow \vec{w} \cdot \vec{v} = 0 \quad (42)$$

When a vector having the indeterminate elements of the terms of the polynomial $f(x_0, ..., x_{H-1})$ as elements is expressed by

$$\vec{w} = (w_1, ..., w_n)$$

and a vector having the coefficients of the terms of the polynomial $f(x_0, ..., x_{H-1})$ as elements is expressed by

$$\vec{v} = (v_1, ..., v_n)$$

whether the polynomial $f(x_0, ..., x_{H-1})$ indicating a logical expression is zero is equivalent to whether the inner product of the vector $\vec{w}$ and the vector $\vec{v}$ is zero.
For example, when the following expressions are used instead of Expressions (39) and (40),

$$\vec{w} = (w_1, ..., w_n) = (x^0, ..., x^{n-1}) \quad (43)$$

$$\vec{v} = (v_1, ..., v_n) = (\theta_0, ..., \theta_{n-1}) \quad (44)$$

whether the polynomial f(x) indicating a logical expression is zero is equivalent to whether the inner product in Expression (41) is zero.

[0139] In inner product predicate encryption, one of the vectors $\vec{v} = (v_1, ..., v_n)$ and $\vec{w} = (w_1, ..., w_n)$ is used as attribute information and the other is used as predicate information. One of the attribute information and predicate information is embedded in ciphertext and the other is embedded in key information. For example, an n-dimensional vector $(\theta_0, ..., \theta_{n-1})$ is used as predicate information, another n-dimensional vector $(x^0, ..., x^{n-1})$ is used as attribute information, one of the attribute information and predicate information is embedded in ciphertext, and the other is embedded in key information. It is assumed in the following description that an n-dimensional vector embedded in key information is $\vec{w} = (w_1, ..., w_n)$ and another n-dimensional vector embedded in ciphertext is $\vec{v} = (v_1, ..., v_n)$. For example,

$$\text{Predicate information:} \quad \vec{w} = (w_1, ..., w_n) = (\theta_0, ..., \theta_{n-1})$$

$$\text{Attribute information:} \quad \vec{v} = (v_1, ..., v_n) = (x^0, ..., x^{n-1})$$

Alternatively,

$$\text{Predicate information:} \quad \vec{v} = (v_1, ..., v_n) = (\theta_0, ..., \theta_{n-1})$$

$$\text{Attribute information:} \quad \vec{w} = (w_1, ..., w_n) = (x^0, ..., x^{n-1})$$

[Basic configuration of inner product predicate encryption]

[0140] The basic configuration of a key encapsulation mechanism (KEM) using inner product predicate encryption will be described below. This configuration includes Setup(1^k), GenKey(MSK, $\vec{w}$), Enc(PA, $\vec{v}$), and Dec(SKw, C_2).

«Setting up Setup(1^k)>>

[0141] Input: Security parameter k
Output: Master key information MSK, public parameter PK
In an example of Setup(1^k), a security parameter k is used as n, an (n + 1) row by (n + 1) column matrix A having an (n + 1)-dimensional basis vector a_i (i = 1, ..., n + 1) as elements, an (n + 1) row by (n + 1) column matrix A* having a basis vector a_i^* (i = 1, ..., n + 1) as elements, and (n + 1) row by (n + 1) column matrixes X and X* used for coordinate conversion are selected. Then, an (n + I)-dimensional basis vector b_i (i = 1, ..., n + 1) is calculated through coordinate conversion by Expression (22), and an (n + 1)-dimensional basis vector b_i^* (i = 1, ..., n + 1) is calculated through coordinate conversion by Expression (24). An (n + 1) row by (n + 1) column matrix B* having the basis vector b_i^* (i = 1, ..., n + 1) as elements is output as master key information MSK; and vector spaces V and V*, an (n + 1) row by (n + 1) column matrix B having the basis vector b_i (i = 1, ..., n + 1) as elements, the security parameter k, the finite field F_q, the elliptic curve E, the cyclic groups G_1, G_2, and G_T, the generating elements g_1, g_2, and g_T, the bilinear function e, and others are output as a public parameter PK.

<<Key information generation GenKey(MSK, $w^{\rightarrow}$)>>

[0142] Input: Master key information MSK, vector $w^{\rightarrow}$
Output: Key information D* corresponding to vector $w^{\rightarrow}$
In an example of GenKey(MSK, $w^{\rightarrow}$), $\alpha \in F_q$ is selected from the finite field F_q. Then, the matrix B*, which is the master key information MSK, is used to generate and output key information D* corresponding to the vector $w^{\rightarrow}$ in the following way.

$$D^* = \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^* \in G_2^{n+1} \qquad (45)$$

If it is difficult to solve a discrete logarithmic problem on the cyclic group G_2, it is difficult to separate and extract the components of $w_\mu \cdot b_\mu^*$ and b_{n+1}^*.

<<Encryption Enc(PA, $v^{\rightarrow}$)>>

[0143] Input: Public parameter PK, vector $v^{\rightarrow}$
Output: Ciphertext C_2, common key K
In an example of Enc(PA, $v^{\rightarrow}$), a common key K and a random number υ_1, which is an element of the finite field F_q, are generated. Then, the public parameter PK, such as the matrix B, an element υ_2 corresponding to a value that includes the common key K, in the finite field F_q, the vector $v^{\rightarrow}$, and the random number υ_1 are used to generate ciphertext C_2 in the following way.

$$C_2 = \upsilon_1 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1} \in G_1^{n+1} \qquad (46)$$

The ciphertext C_2 and the common key K are output. An example of the common key K is $g_T^{\tau \cdot \upsilon 2} \in G_T$, where u2 means υ_2. An example of τ is 1_F, as described above. If it is difficult to solve a discrete logarithmic problem on the cyclic group G_1, it is difficult to separate and extract the components of $v\mu \cdot b\mu$ and $\upsilon_2 \cdot b_{n+1}$.

<<Decryption and key sharing Dec(SKw, C_2)>>

[0144] Input: Key information D_1^* corresponding to vector $w^{\rightarrow}$, ciphertext C_2
Output: Common key K
In an example of Dec(SKw, C_2), the ciphertext C_2 and the key information D_1^* are input to the bilinear function e of Expression (2). Then, from the characteristics of Expressions (3) and (26), the following is satisfied.

$$\begin{aligned} e(C_2, D^*) &= e(\upsilon_1 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1}, \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^*) \\ &= e(\upsilon_1 \cdot v_1 \cdot b_1, \alpha \cdot w_1 \cdot b_1^*) \cdot \ldots \cdot e(\upsilon_1 \cdot v_n \cdot b_n, \alpha \cdot w_n \cdot b_n^*) \\ &\quad \times e(\upsilon_2 \cdot b_{n+1}, b_{n+1}^*) \\ &= e(b_1, b_1^*)^{\upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot e(b_n, b_n^*)^{\upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot e(b_{n+1}, b_{n+1}^*)^{\upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot g_T^{\tau \cdot \upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot v^{\rightarrow} \cdot w^{\rightarrow}} \cdot g_T^{\tau \cdot \upsilon_2} \end{aligned} \qquad \cdots(47)$$

When the inner product $w^{\rightarrow} \cdot v^{\rightarrow}$ is zero, Expression (47) can be changed to the following.

$$e(C_2, D^*) = g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot 0} \cdot g_T^{\tau \cdot \upsilon_2} = g_T^{\tau \cdot \upsilon_2} \quad \cdots(48)$$

From this result, the common key K is generated and output. An example of the common key K is $g_T^{\tau \cdot \upsilon 2} \in G_T$.

[0145] The (n + 1)-dimensional basis vectors are used to configure the algorithm. The dimension is not limited to (n + 1). An (n + Ξ)-dimensional basis vector bi* (i = 1, ..., n + Ξ) may be used to configure the algorithm, were Ξ is a predetermined integer equal to two or more. In that case, Expressions (49) can be used instead of Expression (45), and Expression (50) can be used instead of Expression (46), where υ_i is a constant or a variable (such as a random number).

$$D^* = \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + \sum_{\iota=n+1}^{n+\Xi} \upsilon_\iota \cdot b_\iota^* \in G_2^{n+\Xi} \quad (49)$$

$$C_2 = \upsilon_1 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \sum_{\iota=2}^{\Xi+1} \upsilon_\iota \cdot b_{\iota+n+1} \in G_1^{n+\Xi} \quad (50)$$

[0146] The following expression may be used as Expression (45).

$$D^* = \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + \upsilon_{n+1} \cdot b_{n+1}^* \in G_2^{n+1}$$

In addition, the input information may be switched. Specifically, w is replaced with v in Expression (45) and v is replaced with w in Expression (46).

[0147] Next, description will be given of embodiments according to a first aspect of the present invention which relate to a cryptographic communication technology that is based on functional encryption (predicate encryption is adopted as an example of the functional encryption) and that can operate flexibly. Note that expression numbers are newly assigned below.

(First embodiment according to first aspect)

[0148] A first embodiment according to the first aspect of the present invention will be described below with reference to Fig. 1 to Fig. 17.

[0149] As shown in Fig. 1, a cryptographic system 1 includes a plurality of client apparatuses 10 and 30, one or a plurality of key generation apparatuses 20, one or a plurality of user information management apparatuses 40 (hereafter each called a management apparatus), conversion rule information pair management apparatuses 50 (hereafter each called a registration apparatus), one or a plurality of maintenance apparatuses 80, and one or a plurality of authentication apparatuses 90. These apparatuses can communicate with each other through a communication network 5, such as the Internet.

[0150] The client apparatuses function as encryption apparatuses or decryption apparatuses based on their processing functions. In the light of their functions, the client apparatuses are called encryption apparatuses 10 or decryption apparatuses 30. The cryptographic system 1 may include client apparatuses that function only as encryption apparatuses and/or client apparatuses that function only as decryption apparatuses.

[0151] In the cryptographic system 1, encryption and decryption are performed using predicate encryption. In the first aspect of the present invention, the predicate encryption algorithm to be used is not limited, and the predicate encryption algorithm disclosed in Non-patent literature 2, for example, may be used. In the first embodiment of the first aspect, a predicate encryption algorithm of KEM (the key encapsulation mechanism) type will be used.

[0152] A cryptographic communication method used in the cryptographic system 1 will be described with reference to Figs. 2, 3, 4, 6, 8, and 10. See Figs. 5, 7, and 9 for the functional structure of each apparatus.

«Preparation process»

[0153] A parameter generation unit (not shown) of the key generation apparatus 20 generates a private key and an entry used in the predicate encryption algorithm (step S1). The entry includes a public parameter (abbreviated as a

public P in the figures) used in the predicate encryption algorithm, the address of the key generation apparatus 20, a list of policies that can be used by the key generation apparatus 20, and a list of schemas that can be used by the key generation apparatus 20.

[0154] The public parameter includes, for example, generating elements g_1, g_2, and g_T of cyclic groups G_1, G_2, and G_T having an order q, a non-degenerate bilinear mapping e: $G_1 \times G_2 \rightarrow G_T$ (where $e(g_1, g_2) = g_T$), the order q, and the orthogonal basis B of an (n + 1) dimensional vector space V. The private key includes the orthogonal basis B* of a dual vector space V*. When the algebraic structure is a finite field F_q, q is a prime number or a power of a prime number. The bilinear mapping e is, for example, Tate pairing or Weil pairing.

[0155] The orthogonal basis B and the orthogonal basis B* will be described next. It is assumed that an arbitrary element of the (n + 1) dimensional vector space V is expressed as an element of an (n + 1) dimensional direct product G_1^{n+1} of the cyclic group G_1, as shown in Expression (1). An arbitrary element of the (n + 1) dimensional vector space V can also be expressed by using the canonical basis A of the (n + 1) dimensional vector space V, as shown in Expression (2), where a_i is an element of the (n + 1) dimensional direct product G_1^{n+1}, z_i is an element of an (n + 1) dimensional direct product F_q^{n+1}, and 1 indicates an additive identity.

$$V : (g_1^{z1}, \cdots, g_1^{z_{n+1}}) \in G_1^{n+1} \qquad (1)$$

$$V : z_1 a_1 + \cdots + z_{n+1} a_{n+1} \qquad (2)$$

$$A = (a_1, \cdots, a_{n+1}) = \begin{pmatrix} g_1 & 1 & \cdots & 1 \\ 1 & g_1 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & g_1 \end{pmatrix}, \quad a_i \in G_1^{n+1}$$

$$z_i \in F_q^{n+1}$$

[0156] The orthogonal basis B is obtained by applying an (n + 1) dimensional square matrix X to the canonical basis A, as shown in Expression (3), where symbol T indicates transposition. The matrix X is kept secret as the private key.

$$B = X \cdot A \qquad (3)$$

$$B = {}^T(b_1, \cdots, b_{n+1})$$

$$X = {}^T(x_1, \cdots, x_{n+1}) = (\chi_{ij})_{(n+1)\times(n+1)}, \quad \chi_{ij} \in F_q$$

$$x_i = (\chi_{i1}, \cdots, \chi_{i(n+1)})$$

$$b_i = \sum_{j=1}^{n+1} \chi_{ij}\, a_j = (g_1{}^{x_{i1}}, \cdots, g_1{}^{x_{i(n+1)}})$$

[0157] It is also assumed that an arbitrary element of the dual vector space V* corresponding to the vector space V is expressed as an element of an (n + 1) dimensional direct product $G_2{}^{n+1}$ of the cyclic group G_2, as shown in Expression (4). An arbitrary element of the dual vector space V* can also be expressed by using the canonical basis A* of the dual vector space V*, as shown in Expression (5), where a_i* is an element of the (n + 1) dimensional direct product $G_2{}^{n+1}$, y_i* is an element of the (n + 1) dimensional direct product $F_q{}^{n+1}$, and 1 indicates an additive identity.

$$V^* : (g_2{}^{y_1}, \cdots, g_2{}^{y_{n+1}}) \in G_2{}^{n+1} \qquad (4)$$

$$V^* : y_1 a_1^* + \cdots + y_{n+1} a_{n+1}^* \qquad (5)$$

$$A^* = \left(a_1^*, \cdots, a_{n+1}^*\right) = \begin{pmatrix} g_2 & 1 & \cdots & 1 \\ 1 & g_2 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & g_2 \end{pmatrix}, \quad a_i^* \in G_2{}^{n+1}$$

$$y_i \in F_q{}^{n+1}$$

[0158] The orthogonal basis B* is obtained by applying an (n + 1) dimensional square matrix $^T(X^{-1})$ to the canonical basis A*, as shown in Expression (6), where symbol E indicates a unit matrix.

$$B^* = {}^T(X^{-1}) \cdot A^* \qquad (6)$$

$$B^* = {}^T(b_1^*, \cdots, b_{n+1}^*)$$

$$b_i^* = \left(g_2{}^{x_{i1}^*}, \cdots, g_2{}^{x_{i(n+1)}^*} \right)$$

$$X \cdot {}^T(X^*) = E, \qquad X^* = {}^T(X^{-1})$$

[0159] The schema list will be described next. A pair of conversion rule information items is called a schema pair (see Figs. 11 to 13): one of the conversion rule information items is information (attribute conversion rule information, or attribute schema) that prescribes a conversion rule for converting information that designates an attribute (attribute designation information, that is, information that identifies an attribute such as a name or a date of birth specifically and

uniquely, also called an attribute value) to attribute information used in the predicate encryption algorithm, and the other of the conversion rule information items is information (predicate (logical expression) conversion rule information, or predicate (logical expression) schema) that prescribes a conversion rule for converting information that designates a predicate (logical expression) (predicate (logical expression) designation information, that is, information that specifies a condition related to an attribute, such as an age or an authority specifically by a logical expression, also called a propositional function) to predicate information (logic information) used in the predicate encryption algorithm. A set (data list) of one or a plurality of schema pairs is called a schema list. Each key generation apparatus 20 can determine a schema list in a desired manner. Each data item included in each schema in the schema list is written, for example, in XML (the extensible Markup Language) or ASN.1 (the Abstract Notation Number One).

[0160] An example of the attribute schema shown in Fig. 12 will be described below. User attribute designation information (attribute value) is associated with an attribute name and a data type. In the example shown in Fig. 12, a data type 'character string' is specified for an attribute name 'emaill', and the attribute name 'email1' and the data type 'character string' are associated with an attribute value 'XXX@XXX.ntt.co.jp', for example.

[0161] The attribute schema prescribes a conversion rule in which an element number is associated with an attribute name and a type conversion function. In the example shown in Fig. 12, an element number '1' is associated with an attribute name 'blood type' and a type conversion function, for example. The type conversion function corresponding to the element number '1' converts the attribute value to 0 when the attribute value of the blood type is 'O', to 1 when the attribute value of the blood type is 'A', to 2 when the attribute value of the blood type is 'B', and to 3 when the attribute value of the blood type is 'AB'. Element numbers '2' and '3' are associated with an attribute name "date of birth" and type conversion functions. The type conversion functions corresponding to the element numbers '2' and '3' convert the year of the attribute value of the date of birth to the value of a hash function having the year as the input for the element number '2' and the month and day of the attribute value of the date of birth to the value of the hash function having the month and day as the input for the element number '3'.

[0162] When the example attribute schema shown in Fig. 12 is applied to the example attribute designation information (attribute value) of a user shown in Fig. 12, example attribute information (vector information) shown in Fig. 12 is obtained. This attribute information can be regarded as a vector by arranging the outputs of the type conversion functions by using the element numbers of the attribute schema as the element numbers of the vector.

In general, according to the functional encryption, a plurality of pieces of attribute information can be designated at the time of encryption. For example, an attribute schema is applied to a plurality of pieces of attribute designation information, whereby a plurality of pieces of attribute information can be obtained. Alternatively, a plurality of attribute schemas may be applied to one piece of attribute designation information, whereby a plurality of pieces of attribute information may be obtained.

[0163] In the above description, the outputs of the type conversion functions are integers and the output values of the hash function. In reality, the outputs of the type conversion functions depend on the predicate encryption algorithm and are, for example, elements of the finite field F_q.

[0164] An example of the predicate schema shown in Fig. 13 will be described below. As predicate designation information, logic expressions that specify conditions for attributes are given. In the example shown in Fig. 13, the predicate designation information of 'name = Taro Tanaka AND age = 20 or more' which means the attribute value of an attribute name 'name' is 'Taro Tanaka' and the attribute value of an attribute name 'age' is '20 or more" is given.

[0165] The predicate schema prescribes a conversion rule in which an element number is associated with an attribute name and a type conversion function. In the example shown in Fig. 13, an element number '1' is associated with an attribute name 'blood type' and a type conversion function, for example. The type conversion function corresponding to the element number '1' converts the attribute value to 0 when the attribute value of the blood type is 'O', to 1 when the attribute value of the blood type is 'A', to 2 when the attribute value of the blood type is 'B', and to 3 when the attribute value of the blood type is 'AB'. Element numbers '2' and '3' are associated with an attribute name 'date of birth' and type conversion functions. The type conversion functions corresponding to the element numbers '2' and '3' convert the year of the attribute value of the date of birth to the value of a hash function having the year as the input for the element number '2' and the month and day of the attribute value of the date of birth to the value of the hash function having the month and day as the input for the element number '3'.

[0166] When the example predicate schema shown in Fig. 13 is applied to the example predicate designation information shown in Fig. 13, example predicate information (vector information) shown in Fig. 13 is obtained. Specifically, in this example, the predicate schema is applied to the predicate designation information to obtain a multivariate polynomial f having variables corresponding to the element numbers, and the multivariate polynomial f is converted to vector information to obtain predicate information (vector information). This process will be described below by using the example predicate designation information shown in Fig. 13. When the predicate schema is applied to the predicate designation information of 'name = Taro Tanaka AND age = 20 or more', the output value 'Hash (Taro Tanaka)' of the type conversion function corresponding to an element number '0' and the output value '1' of the type conversion function corresponding to an element number '23' are obtained. A polynomial with a degree of one with respect to a variable X_0

corresponding to the element number '0', which has the output value 'Hash (Taro Tanaka)' of the type conversion function corresponding to the element number '0' as a zero, and a polynomial with a degree of one with respect to a variable X_{23} corresponding to the element number '23', which has the output value '1' of the type conversion function corresponding to the element number '23' as a zero, are linearly combined to obtain a multivariate polynomial $f = r_1(X_0 - H(\text{Taro Tanaka})) + r_2(X_{23} - 1)$, where r_1 and r_2 are random numbers. Then, this multivariate polynomial f is expanded and the coefficients of the terms are arranged to convert the multivariate polynomial f to vector information. The example of the predicate information (vector information) shown in Fig. 13 is thus obtained.

In general, according to the functional encryption, a plurality of pieces of predicate information can be designated at the time of encryption. For example, a predicate schema is applied to a plurality of pieces of predicate designation information, whereby a plurality of pieces of predicate information can be obtained. Alternatively, a plurality of predicate schemas may be applied to one piece of predicate designation information, whereby a plurality of pieces of predicate information may be obtained.

[0167] In the above description, the outputs of the type conversion functions are integers or the output values of the hash function. In reality, the outputs of the type conversion functions depend on the predicate encryption algorithm and are, for example, elements of the finite field F_q.

[0168] Both schemas constituting a schema pair need to have the same combinations of attribute names and type conversion functions, the same data types of attribute values to be input, and the like.

[0169] The policy list will be described next with reference to Fig. 14. Information that identifies either the attribute schema or the predicate schema is called policy information (hereafter called just policy). A data list in which the policy is written is called a policy list. When the key generation apparatus 20 uses both the attribute schema and the predicate schema, two types of policies are prepared: Cipher_Text_Policy and Key_Policy. When the key generation apparatus 20 uses only the attribute schema, just one type of policy is prepared: Key_Policy. When the key generation apparatus 20 uses only the predicate schema, just one type of policy is prepared: Cipher_Text_Policy. The policy is written, for example, with XML (the extensible Markup Language) or ASN.1 (the Abstract Notation Number One). The key generation apparatus 20 can freely determine the policy target: only the attribute schema, only the predicate schema, or both the attribute schema and the predicate schema.

In general, according to the functional encryption, as described above, the plurality of different attribute schemas are applied to one piece of attribute designation information, whereby the plurality of pieces of attribute information can be obtained. In such a case, the plurality of attribute schemas are designated in advance as the policy. The plurality of different predicate schemas are applied to one piece of predicate designation information, whereby the plurality of pieces of predicate information can be obtained. In such a case, the plurality of predicate schemas are designated in advance as the policy.

[0170] After the process of step S1, a transmitter unit of the key generation apparatus 20 sends the entry to the authentication apparatus 90, and a receiver unit of the authentication apparatus 90 receives the entry (step S2). A signature assigning unit (not shown) of the authentication apparatus 90 assigns an electronic signature to the entry with, for example, a conventional method (step S3), a transmitter unit of the authentication apparatus 90 sends the entry with the signature to the key generation apparatus 20, and a receiver unit of the key generation apparatus 20 receives the entry with the signature (step S4). Then, the transmitter unit of the key generation apparatus 20 sends the entry with the signature to the maintenance apparatus 80, and a receiver unit of the maintenance apparatus 80 receives the entry with the signature (step S5).

[0171] A transmitter unit of the maintenance apparatus 80 sends a search query, which includes information (such as address) identifying the key generation apparatus 20, to the registration apparatus 50, and a receiver unit of the registration apparatus 50 receives the search query (step S6). A searching unit (not shown) of the registration apparatus 50 searches for the registered content (entry) concerning the key generation apparatus 20 (step S7), a transmitter unit of the registration apparatus 50 sends a search result, which includes whether registration has been made and the registered content, to the maintenance apparatus 80, and the receiver unit of the maintenance apparatus 80 receives the search result (step S8).

[0172] A checking unit (not shown) of the maintenance apparatus 80 compares the entry with the signature received in the process of step S5 with the search result received in the process of step S8 to check if the entry has already been registered (step S9). If it is determined that the entry has not yet been registered, the transmitter unit of the maintenance apparatus 80 sends the entry with the signature to the registration apparatus 50, and the receiver unit of the registration apparatus 50 receives the entry with the signature (step S10). A registration unit (not shown) of the registration apparatus 50 stores the entry with the signature in a storage unit of the registration apparatus 50 in association with the key generation apparatus 20 (step S11). The transmitter unit of the registration apparatus 50 sends the registration result to the maintenance apparatus 80, and the receiver unit of the maintenance apparatus 80 receives the registration result (step S12). The transmitter unit of the maintenance apparatus 80 sends the registration result to the key generation apparatus 20, and the key generation apparatus 20 receives the registration result (step S13).

[0173] When a plurality of key generation apparatuses 20 are provided, each of the plurality of key generation apparatuses 20 separately performs the processes of step S1 to step S13. For example, each key generation apparatus

specifies a public parameter and a private key. However, this does not prevent each key generation apparatus from having a common public parameter and a common private key. The key generation apparatuses may register their entries in the same registration apparatus 50 or in different registration apparatuses 50.

[0174] When the private key and the entry are specified in advance and the entry is registered in the registration apparatus 50 in advance, the processes from step S1 to step S13 may be omitted.

[0175] The authentication apparatus 90 and the maintenance apparatus 80 may be the same hardware entity. The cryptographic system 1 may have a system structure having no maintenance apparatus 80, no authentication apparatus 90, or no maintenance apparatus 80 and no authentication apparatus 90 when authentication is not required for registering an entry or when it is guaranteed unity of the entry is registered in the registration apparatus 50.

[0176] The description of «the preparation process» ends here.

«Encryption process»

[0177] Under the control of a controller unit, not shown, a transmitter unit 14 of the encryption apparatus 10 sends a search query to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S14). The searching unit of the registration apparatus 50 searches some or all of the entries registered in the storage unit of the registration apparatus 50 and chooses any one entry (step S15). The transmitter unit of the registration apparatus 50 sends the entry to the encryption apparatus 10, and a receiver unit of the encryption apparatus 10 receives the entry (step S16). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 11 of the encryption apparatus 10.

[0178] When the encryption apparatus 10 has the public parameter, schema list, policy list, and address of each key generation apparatus 20 in advance, the processes of steps S 14 to S16 are omitted. It should be noted that the cryptographic system 1 may have no registration apparatus 50.

[0179] A first predicate logic information acquisition unit 12 of the encryption apparatus 10 reads the input information, the policy, and the schemas from the memory 11 and obtains attribute information (hereafter called first attribute information) and predicate information (hereafter called first predicate information) (step S17a). Details of this process will be described below with reference to Figs. 12 and 13.

[0180] When the schema list has a plurality of schema pairs, one schema pair is selected based on the usage or the like. The user of the encryption apparatus 10 may select a schema pair and input designation information thereof. Alternatively, the first predicate logic information acquisition unit 12 may select a schema pair according to a predetermined rule.

[0181] According to whether the input information is attribute designation information or predicate designation information, one of the schemas is selected together with the policy. The user of the encryption apparatus 10 may select the policy and one of the schemas and input designation information thereof. Alternatively, the first predicate logic information acquisition unit 12 may select the policy and one of the schemas according to a predetermined rule. When only one type of policy is prepared in the key generation apparatus 20, one schema of the schema pair is selected according to the policy. If the selected schema does not correspond to the type of the input information, a schema pair needs to be selected again from the schema list or an entry needs to be provided by the registration apparatus 50 again.

[0182] The input information may be information inputted by the user of the encryption apparatus 10 or information acquired by an acquisition unit (not shown) of the encryption apparatus 10 from a storage medium such as an IC card 39.

[0183] Then, the first predicate logic information acquisition unit 12 uses the schema selected from the schema pair according to the policy to obtain the first attribute information or the first predicate information from the input information. When the policy is Key_Policy and the selected schema is an attribute schema, the first attribute information is obtained. When the policy is Cipher_Text_Policy and the selected schema is a predicate schema, the first predicate information is obtained. The first attribute information and the first predicate information are one or a plurality of vector information having elements of the finite field F_q as components in the first embodiment according to the first aspect (see Figs. 11 to 13). The schema is used to extract or arrange necessary attribute values from the input information.

[0184] Next, an encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, an orthogonal basis B (substantial public key) included in the public parameter read from the memory 11, and plaintext M to obtain a common key K, encryption information C_1, and ciphertext C_2 (steps S 17b and S17c). Details of these processes will be described below. When the first embodiment of the first aspect is dedicated to the delivery of the common key K, it is not necessary to generate the ciphertext C_2.

[0185] A first encryption unit 13a generates random numbers r and p which are elements of the finite field Fq according to the predicate encryption algorithm, specifies the common key K as shown by Expression (7), and obtains the encryption information C_1 according to Expression (8) (step S17b), where H indicates, for example, a hash function. In this example, the first attribute information v is used. To use the first predicate information, v needs to be replaced with w in Expression

(8). In this example, the encryption information C_1 corresponds to p used to generate the common key K. The encryption information C_1 may correspond to the common key K.

$$K = H(g_T{}^{\rho}) \qquad (7)$$

$$C_1 = r\sum_{i=1}^{n} v_i b_i + \rho b_{n+1} \qquad (8)$$

[0186] Next, the second encryption unit 13b uses the common key K and the plaintext M to obtain the ciphertext C_2 according to Expression (9) (step S17c). An encryption method Enc_k that uses the private key can be a known method. For example, it may be the method disclosed in Non-patent literature 1. As described earlier, when the first embodiment of the first aspect is dedicated to the delivery of the common key K, the process of step S17c is omitted. In other words, the encryption apparatus 10 has even the function of the second encryption unit 13b but does not perform the process of step S17c.

$$C_2 = Enc_K(M) \qquad (9)$$

[0187] Next, under the control of the controller unit, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1 and the ciphertext C_2 (if necessary), together with the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 11 (step S 17d). The transmitter unit 14 of the encryption apparatus 10 then sends the encrypted message to the decryption apparatus 30, and a receiver unit of the decryption apparatus 30 receives the encrypted message (step S18).

[0188] The description of «the encryption process» ends here.

«Decryption process»

[0189] Under the control of a controller unit, not shown, a transmitter unit 34 of the decryption apparatus 30 sends a search query that includes the address of the key generation apparatus, the address being included in the encrypted message, to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S19). The searching unit of the registration apparatus 50 searches for the entry of the key generation apparatus specified by the address and selects it (step S20). The transmitter unit of the registration apparatus 50 sends the entry of the search result to the decryption apparatus 30, and the receiver unit of the decryption apparatus 30 receives the entry (step S21). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 31 of the decryption apparatus 30.

[0190] When the decryption apparatus 30 has the public parameter, schema list, policy list, and address of each key generation apparatus 20 in advance, the processes of steps S 19 to S21 are omitted. In that case, the decryption apparatus 30 searches the memory 31 for the entry of the key generation apparatus corresponding to the address included in the encrypted message and retrieves it.

[0191] Under the control of the controller unit, a verification unit (not shown) of the decryption apparatus 30 verifies that the schema pair and the policy included in the encrypted message are included in the schema list and the policy list included in the entry obtained from the registration apparatus 50 (step S22a). If this verification fails, the process ends with a decryption processing failure (step S22g).

[0192] When the verification succeeds, an acquisition unit 32 of the decryption apparatus 30 reads the attribute designation information or the predicate designation information corresponding to the user of the decryption apparatus 30 from a storage medium such as the IC card 39 (step S22f). Whether the attribute designation information or the predicate designation information is read depends on the policy included in the encrypted message. More specifically, the read designation information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the encrypted message. When the policy is Cipher_Text_Policy, the acquisition unit 32 reads the attribute designation information from the storage medium. When the policy is Key_Policy, the acquisition unit 32 reads the predicate designation information from the storage medium. The read designation information is hereafter called user information. The acquisition unit 32 of the decryption apparatus 30 may read from the management

apparatus 40 the attribute designation information or the predicate designation information corresponding to the user of the decryption apparatus 30, in the same way as in «a user information acquisition process» in the key generation apparatus 20, described later. In the first embodiment of the first aspect, the process of step S22f may be omitted. When the decryption apparatus 30 has the attribute designation information and the predicate designation information corresponding to the user in advance, either the attribute designation information or the predicate designation information serves as user information, according to the policy.

[0193] Next, the verification unit of the decryption apparatus 30 verifies that the decryption apparatus 30 has the decryption key to be used to decrypt the encryption information included in the encryption message (step S22b).

[0194] The decryption apparatus 30 stores a decryption key table in the memory 31. In the decryption key table, as shown in Fig. 15, for example, the identifier of each key generation apparatus is associated with the public parameter, the schema pair, the decryption key target, the predicate designation information, and the decryption key. The verification unit verifies that the decryption apparatus 30 has the decryption key corresponding to the identifier of the key generation apparatus determined from the address included in the encrypted message, to the public parameter, to the schema pair, and to the decryption key target (corresponding to the content of the policy identifying one schema paired with the other schema identified by the policy included in the encrypted message). When the decryption apparatus 30 has the decryption key, the process of step S29 will be performed. If the decryption apparatus 30 does not have the decryption key, the process of step S23 will be performed.

[0195] The description of «the decryption process» is temporarily halted here and «a key generation process» will be described below.

[0196] If the decryption apparatus 30 does not have the decryption key, the transmitter unit 34 of the decryption apparatus 30 generates, under the control of the controller unit, a key request message that includes the public parameter, the policy, the schema pair, the user information (if any), and the authentication information, all of these items being read from the memory 31. The authentication information includes, for example, the ID of the user and a password. The transmitter unit 34 of the decryption apparatus 30 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message (step S23). The received key request message is stored in a memory 21 of the key generation apparatus 20.

[0197] Under the control of a controller unit, a verification unit (not shown) of the key generation apparatus 20 verifies that the schema pair and the policy included in the key request message are included in the schema list and the policy list included in the entry owned by the key generation apparatus 20 (for example, the entry generated in step S1) and that the public parameter included in the key request message is identical to the public parameter of the key generation apparatus 20 (step S24a). If this verification fails, the process ends with a key generation process failure (step S24g). When the authentication information is included in the key request message, the authentication information is also verified in the process of step S24a. The key generation apparatus 20 stores an authentication table in the memory 21. In the authentication table, as shown in Fig. 16, for example, each user ID is associated with a password. The verification unit verifies that the user ID and the password included in the key request message are identical to the user ID and the password included in the authentication table. If the verification fails, the process of step S24g is performed.

[0198] When this verification succeeds, the verification unit of the key generation apparatus 20 verifies that the key request message includes the user information (step S24b). When the key request message includes the user information, the process of step S24c will be performed. If the key request message does not include the user information, the process of step S25 will be performed. When a method is employed in which a key request message always includes user information, the process of step S24b and «a user information acquisition process», described later, are unnecessary.

[0199] The description of «the key generation process» is temporarily halted here and «the user information acquisition process» will be described below.

[0200] The transmitter unit 24 of the key generation apparatus 20 sends a request that includes the policy and the authentication information (if any) included in the key request message to the management apparatus 40, and the management apparatus 40 receives the request (step S25). The received request is stored in a memory of the management apparatus 40.

[0201] The management apparatus 40 stores an authentication table in the memory. In the same way as in the authentication table described above, the user ID is associated with the password in this authentication table (see Fig. 16). A verification unit (not shown) of the management apparatus 40 verifies that the user ID and the password included in the request are identical to the user ID and the password included in the authentication table.

[0202] When this verification succeeds, a searching unit (not shown) of the management apparatus 40 searches a user information table stored in the memory for the attribute designation information or the predicate designation information according to the policy included in the request (step S26). The user information table includes, for example, a first table formed of each user ID, and an attribute name and attribute designation information associated with the user ID, and a second table formed of the user ID and predicate designation information associated with the user ID (see Fig. 17). Whether the attribute designation information or the predicate designation information is read is determined by

the policy included in the request. More specifically, the read information corresponds to the content of one policy identifying the schema paired with the other schema identified by the policy included in the request. When the policy is Cipher_Text_Policy, the searching unit reads the attribute designation information corresponding to the user ID included in the request from the first table. When the policy is Key_Policy, the searching unit reads the predicate designation information corresponding to the user ID included in the request from the second table. The read designation information is hereafter called user information.

[0203] Under the control of a controller unit, a transmitter unit of the management apparatus 40 sends the user information to the key generation apparatus 20, and the receiver unit of the key generation apparatus 20 receives the user information (step S27). The received user information is stored in the memory 21 of the key generation apparatus 20.

[0204] The description of «the user information acquisition process» ends here, and the description of «the key generation process» will be resumed.

[0205] When the key generation apparatus 20 already has the user information or receives the user information through the user information acquisition process (step S27), a second predicate logic information acquisition unit 23 of the key generation apparatus 20 reads the policy, the schema pair, the public parameter, and the user information from the memory 21, and obtains attribute information (hereafter called second attribute information) or predicate information (second predicate information) from the user information (step S24c). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the first embodiment of the first aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13). The schema is used to extract and arrange necessary attribute values from the input information.

[0206] Next, a key generation unit 25 of the key generation apparatus 20 generates a random number α that is an element of the finite field F_q, based on the public parameter q according to the predicate encryption algorithm, and uses the random number α, the second attribute information $v_{(p)} = (V_{(p)1}, ..., V_{(p)n})$ or the second predicate information $w_{(p)} = (w_{(p)1}, ..., w_{(p)n})$ read from the memory 21, and a private key B* of the key generation apparatus to obtain a decryption key R according to Expression (10) (step S24d). The second predicate information $w_{(p)}$ is used in this example because the input information used in the encryption process is the attribute designation information. When the input information is the predicate designation information, the second attribute information $v_{(p)}$ is used. Therefore, $w_{(p)}$ needs to be replaced with $v_{(p)}$ in Expression (10).

$$R = \alpha \sum_{i=1}^{n} w_{(p)i} b_i^* + b_{n+1}^* \qquad (10)$$

[0207] Next, under the control of the controller unit, the transmitter unit 24 of the key generation apparatus 20 sends the decryption key R to the decryption apparatus 30, and the receiver unit of the decryption apparatus 30 receives the decryption key R (step S28). The received decryption key R is stored in the memory 31 of the decryption apparatus 30.

[0208] The description of «the key generation process» ends here, and the description of «the decryption process» will be resumed.

[0209] When the decryption apparatus 30 already has the decryption key or receives the decryption key through the key generation process (step S28), a decryption unit 33 of the decryption apparatus 30 reads the public parameter, the decryption key R, the encryption information C_1, and the ciphertext C_2 (if necessary) from the memory 31, and obtains the common key K and the plaintext M (if necessary) (step S29).

[0210] Details of the process in step S29 will be described below. A first decryption unit 33a reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31, and obtains $e(C_1, R)$ according to the predicate encryption algorithm. As shown in Expression (11), the calculation result depends on the result of the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ taken out from the encryption information C_1 and the decryption key R according to bilinearity when the input information is the attribute designation information. When the input information is the predicate designation information, v needs to be replaced with $v_{(p)}$ and $w_{(p)}$ needs to be replaced with w in Expression (11). The calculation result depends on the result of the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ taken out from the encryption information C_1 and the decryption key R according to bilinearity. In Expression (11), $e(b_i, b_i^*)$ is defined as shown in Expression (12), where δ_{ij} is the Kronecker's delta symbol.

$$e(C_1, R) = e(r\sum_{i=1}^{n} v_i b_i, R) \cdot e(\rho b_{n+1}, R)$$

$$= \prod_{i=1}^{n} e(b_i, b_i^*)^{r\alpha v_i w_{(p)i}} \cdot e(b_{n+1}, b_{n+1}^*)^{\rho}$$

$$= g_T{}^{r\alpha \sum_{i=1}^{n} v_i w_{(p)i}} \cdot g_T{}^{\rho}$$

$$= g_T{}^{r\alpha\, v \cdot w_{(p)}} \cdot g_T{}^{\rho} \qquad (11)$$

$$e(b_i, b_j^*) = \prod_{j=1}^{n+1} e(g_1^{\chi_{ij}}, g_2^{\chi_{ij}^*})$$

$$= g_T{}^{\sum_{j=1}^{n+1} \chi_{ij}\chi_{ij}^*}$$

$$= g_T{}^{x_i \cdot {}^T x_j^*}$$

$$= g_T{}^{\delta_{ij}} \qquad (12)$$

[0211] Therefore, when the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ is zero (or when the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ is zero), the result of calculation in Expression (11), $g_T{}^{\rho}$, is obtained. When the result of calculation, $g_T{}^{\rho}$, is obtained, the first decryption unit 33a of the decryption apparatus 30 obtains the common key K, which is correct, according to Expression (7) (step S22c). When the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ is not zero (or when the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ is not zero), the first decryption unit 33a obtains an incorrect value according to Expression (7). In this example, it is assumed that the hash function H is common to the system or is included in the public parameter. The encryption information C_1 corresponds to the information p used to generate the common key K in this example. When encryption information C_1 corresponds to the common key K, the result of calculation in Expression (11) is the common key K (or incorrect value). In other words, an authorized user of the decryption apparatus 30 has predicate designation information that gives the second predicate information $w_{(p)}$ which makes the canonical inner product with the first attribute information v zero, or attribute designation information that gives the second attribute information $v_{(p)}$ which makes the canonical inner product with the first predicate information w zero.

[0212] Then, a second decryption unit 33b uses the common key K and the ciphertext C_2 to calculate plaintext M according to Expression (13) (step S22d). A decryption method Dec_K that uses the private key corresponds to the encryption method Enc_K. As described earlier, when the first embodiment of the first aspect is dedicated to the delivery of the common key K, the process of step S22d is omitted. More specifically, even if the decryption apparatus 30 has the function of the second decryption unit 33b, it does not perform the process of step S22d.

$$M = Dec_K(C_2) \qquad (13)$$

[0213] If the result of calculation in Expression (11) is an incorrect value, the correct plaintext M cannot be obtained by Expression (13).

[0214] The decryption apparatus 30 may store the decryption key R in the decryption key table. In addition, the

decryption apparatus 30 may store the common key K in the decryption key table.

[0215] The description of «the decryption process» ends here.

(Second embodiment according to first aspect)

[0216] A second embodiment of the first aspect differs from the first embodiment of the first aspect in that the decryption apparatus 30 generates the second attribute information or the second predicate information. Because of this difference, the second embodiment of the first aspect differs in several points from the first embodiment of the first aspect. A description of commonalities between the first and second embodiments of the first aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the first aspect will be made with reference to Figs. 18 to 21.

[0217] The processes of steps S1 to S22b are the same as those in the first embodiment of the first aspect.

[0218] When the decryption key is not possessed in the process of step S22b, a second predicate logic information acquisition unit 35 of the decryption apparatus 30 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S23g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the second embodiment of the first aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0219] After the process of step S23g, the process of step 23 is performed. In this process, the transmitter unit 34 of the decryption apparatus 30 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the decryption apparatus 30 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0220] When the verification succeeds in the process of step S24a, the process of step S24d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the decryption apparatus 30, the function and the process for generating the information are unnecessary, unlike in the first embodiment of the first aspect.

[0221] The processes of steps S28 and S29, to be performed after the process of step S24d, are the same as those in the first embodiment of the first aspect.

(Third embodiment according to first aspect)

[0222] A third embodiment of the first aspect differs from the first embodiment of the first aspect in that the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1. In other words, the predicate encryption algorithm disclosed in Non-patent literature 2, for example, is used in the third embodiment of the first aspect. Because of this difference, the third embodiment of the first aspect differs in several points from the first embodiment of the first aspect. A description of commonalities between the first and third embodiments of the first aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the first aspect will be made with reference to Figs. 22 to 25.

[0223] The processes of steps S1 to S17a are the same as those in the first embodiment of the first aspect. The public parameter and some other information are required by the predicate encryption algorithm of the third embodiment of the first aspect. For specific information required, see Non-patent literature 2, described above, for example.

[0224] In the process of step S17b1, following the process of step S17a, the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1 according to the predicate encryption algorithm (step S17b1).

[0225] After the process of step S17b1, the process of step 17d is performed. In this process, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1, and the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory

31, under the control of the controller unit (step S 17d).

[0226] The processes of steps S18 to S28, following the process of step S17d, are the same as those in the first embodiment of the first aspect.

[0227] In the process of step S22c1, following the process of step S28, the decryption unit 33 of the decryption apparatus 30 reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31 to calculate plaintext M according to the predicate encryption algorithm (step S22c1).

(Fourth embodiment according to first aspect)

[0228] A fourth embodiment of the first aspect corresponds to a combination of the second embodiment of the first aspect and the third embodiment of the first aspect. The fourth embodiment of the first aspect differs from the first embodiment of the first aspect in that (1) the decryption apparatus 30 generates the second attribute information or the second predicate information, and (2) the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1. Because of these differences, the fourth embodiment of the first aspect differs in several points from the first embodiment of the first aspect. A description of commonalities between the first and fourth embodiments of the first aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the first aspect will be made with reference to Figs. 26 and 27.

[0229] The processes of steps S1 to S17a are the same as those in the first embodiment of the first aspect. The public parameter and some other information are required by the predicate encryption algorithm of the fourth embodiment of the first aspect. For specific information required, see Non-patent literature 2, described above, for example.

[0230] In the process of step S17b1, following the process of step S17a, the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1 according to the predicate encryption algorithm (step S17b1).

[0231] After the process of step S17b1, the process of step 17d is performed. In this process, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1, and the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 31, under the control of the controller unit (step S 17d).

[0232] The processes of steps S18 to S22b, following the process of step S17d, are the same as those in the first embodiment of the first aspect.

[0233] When the decryption key is not possessed in the process of step S22b, the second predicate logic information acquisition unit 35 of the decryption apparatus 30 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S23g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the fourth embodiment of the first aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0234] After the process of step S23g, the process of step 23 is performed. In this process, the transmitter unit 34 of the decryption apparatus 30 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the decryption apparatus 30 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0235] When the verification succeeds in the process of step S24a, the process of step S24d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the decryption apparatus 30, the function and the process for generating the information are unnecessary.

[0236] The process of step S28, following the process of step S24d, is the same as that in the first embodiment of the first aspect.

[0237] In the process of step S22c1, following the process of step S28, the decryption unit 33 of the decryption apparatus 30 reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31 to calculate plaintext M according to the predicate encryption algorithm (step S22c1).

[0238] Embodiments according to a second aspect of the present invention, which relate to a cryptographic communication technology that can operate flexibly, that is based on predicate encryption, and that allows encryption information encrypted with the predicate encryption to be distributed will be described next while attention is being paid to the cryptographic communication technology of the first aspect, described above. Since a decryption apparatus has a transfer function in the cryptographic communication technology of the second aspect, encryption information encrypted with the predicate encryption can be distributed.

[0239] The description of the cryptographic communication technology of the second aspect and the description of the cryptographic communication technology of the first aspect have many substantial commonalities, but, to avoid referring to the description of the cryptographic communication technology of the first aspect, the cryptographic communication technology of the second aspect will be described below with overlapping explanations and figures being included as much as possible. Therefore, in both descriptions, identical expression numbers, identical reference numerals assigned to function blocks, and identical reference numerals assigned to steps are used. Because the contexts are different, there should be no risk of confusion.

(First embodiment according to second aspect)

[0240] A first embodiment according to the second aspect of the present invention will be described below with reference to Fig. 28 to Fig. 41.

[0241] As shown in Fig. 28, a cryptographic system 1 according to the second aspect includes a plurality of client apparatuses 10, 30-1, and 30-2, one or a plurality of key generation apparatuses 20, one or a plurality of user information management apparatuses 40 (hereafter each called a management apparatus), conversion rule information pair management apparatuses 50 (hereafter each called a registration apparatus), one or a plurality of maintenance apparatuses 80, and one or a plurality of authentication apparatuses 90. These apparatuses can communicate with each other through a communication network 5, such as the Internet.

[0242] The client apparatuses function as encryption apparatuses or decryption apparatuses based on their processing functions. In the light of their functions, the client apparatuses are called encryption apparatuses 10 or decryption apparatuses. The decryption apparatuses include a first decryption apparatus 30-1 serving as an apparatus for exchanging an encrypted message, described later, with the encryption apparatus 10 and a second decryption apparatus 30-2 that does not perform such an exchange. The cryptographic system 1 according to the second aspect may include client apparatuses that function only as encryption apparatuses and/or client apparatuses that function only as decryption apparatuses.

[0243] In the cryptographic system 1 according to the second aspect, encryption and decryption are performed using predicate encryption. In the second aspect of the present invention, the predicate encryption algorithm to be used is not limited, and the predicate encryption algorithm disclosed in Non-patent literature 2, for example, may be used. In the first embodiment of the second aspect, a predicate encryption algorithm of KEM (the key encapsulation mechanism) type will be used.

[0244] A cryptographic communication method used in the cryptographic system 1 according to the second aspect will be described with reference to Figs. 29, 30, 31, 32, 34, 36, 38, 40, and 41. See Figs. 33, 35, 37, and 39 for the functional structure of each apparatus.

«Preparation process»

[0245] The entire description of «the preparation process» in the first embodiment of the first aspect according to the present invention is incorporated here and a description of «the preparation process» is omitted. See Fig. 29 for the preparation process, Figs. 11 to 13 for schema pairs, and Fig. 14 for policy lists. The description of the preparation process ends here.

«Encryption process»

[0246] Under the control of a controller unit, not shown, a transmitter unit 14 of the encryption apparatus 10 sends a search query to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S14). The searching unit of the registration apparatus 50 searches some or all of the entries registered in the storage unit of the registration apparatus 50 and chooses one entry (step S15). The transmitter unit of the registration apparatus 50 sends the entry to the encryption apparatus 10, and a receiver unit of the encryption apparatus 10 receives the entry (step S16). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 11 of the encryption apparatus 10.

[0247] When the encryption apparatus 10 has the public parameter, schema list, policy list, and address of each key

generation apparatus 20 in advance, the processes of steps S 14 to S16 are omitted. It should be noted that the cryptographic system 1 may have no registration apparatus 50.

[0248] A first predicate logic information acquisition unit 12 of the encryption apparatus 10 reads the input information, the policy, and the schemas from the memory 11 and obtains attribute information (hereafter called first attribute information) and predicate information (hereafter called first predicate information) (step S17a). Details of this process will be described below with reference to Figs. 12 and 13.

[0249] When the schema list has a plurality of schema pairs, one schema pair is selected based on the usage or the like. The user of the encryption apparatus 10 may select a schema pair and input designation information thereof. Alternatively, the first predicate logic information acquisition unit 12 may select a schema pair according to a predetermined rule.

[0250] According to whether the input information is attribute designation information or predicate designation information, one of the schemas is selected together with the policy. The user of the encryption apparatus 10 may select the policy and one of the schemas and input designation information thereof. Alternatively, the first predicate logic information acquisition unit 12 may select the policy and one of the schemas according to a predetermined rule. When only one type of policy is prepared in the key generation apparatus 20, one schema of the schema pair is selected according to the policy. If the selected schema does not correspond to the type of the input information, a schema pair needs to be selected again from the schema list or an entry needs to be provided by the registration apparatus 50 again.

[0251] The input information may be information inputted by the user of the encryption apparatus 10 or information acquired by an acquisition unit (not shown) of the encryption apparatus 10 from a storage medium such as an IC card 39.

[0252] Then, the first predicate logic information acquisition unit 12 uses the schema selected from the schema pair according to the policy to obtain the first attribute information or the first predicate information from the input information. When the policy is Key_Policy and the selected schema is an attribute schema, the first attribute information is obtained. When the policy is Cipher_Text_Policy and the selected schema is a predicate schema, the first predicate information is obtained. The first attribute information and the first predicate information are one or a plurality of vector information having elements of the finite field F_q as components in the first embodiment according to the second aspect (see Figs. 11 to 13). The schema is used to extract or arrange necessary attribute values from the input information.

[0253] Next, an encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, an orthogonal basis B (substantial public key) included in the public parameter read from the memory 11, and plaintext M to obtain a common key K, encryption information C_1, and ciphertext C_2 (steps S 17b and S17c). Details of these processes will be described below. When the first embodiment of the second aspect is dedicated to the delivery of the common key K, it is not necessary to generate the ciphertext C_2.

[0254] A first encryption unit 13a generates random numbers r and p which are elements of the finite field Fq according to the predicate encryption algorithm, specifies the common key K as shown by Expression (7), and obtains the encryption information C_1 according to Expression (8) (step S17b), where H indicates, for example, a hash function. In this example, the first attribute information v is used. To use the first predicate information, v needs to be replaced with w in Expression (8). In this example, the encryption information C_1 corresponds to p used to generate the common key K. The encryption information C_1 may correspond to the common key K.

[0255] Next, the second encryption unit 13b uses the common key K and the plaintext M to obtain the ciphertext C_2 according to Expression (9) (step S17c). An encryption method Enc_k that uses the private key can be a known method. For example, it may be the method disclosed in Non-patent literature 1. As described earlier, when the first embodiment of the second aspect is dedicated to the delivery of the common key K, the process of step S17c is omitted. In other words, the encryption apparatus 10 has even the function of the second encryption unit 13b but does not perform the process of step S17c.

[0256] Next, under the control of the controller unit, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1 and the ciphertext C_2 (if necessary), together with the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 11 (step S 17d). The transmitter unit 14 of the encryption apparatus 10 then sends the encrypted message to the first decryption apparatus 30-1, and a receiver unit of the first decryption apparatus 30-1 receives the encrypted message (step S18). The encryption apparatus 10 is allowed to send an encrypted message to a plurality of first decryption apparatuses 30-1.

[0257] The description of «the encryption process» ends here.

«First decryption process»

[0258] Under the control of a controller unit, not shown, a transmitter unit 34 of the first decryption apparatus 30-1 sends a search query that includes the address of the key generation apparatus, the address being included in the encrypted message, to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S19). The searching unit of the registration apparatus 50 searches for the entry of the key

generation apparatus specified by the address and selects it (step S20). The transmitter unit of the registration apparatus 50 sends the entry of the search result to the first decryption apparatus 30-1, and the receiver unit of the first decryption apparatus 30-1 receives the entry (step S21). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 31 of the first decryption apparatus 30-1.

[0259] When the first decryption apparatus 30-1 has the public parameter, schema list, policy list, and address of each key generation apparatus 20 in advance, the processes of steps S 19 to S21 are omitted. In that case, the first decryption apparatus 30-1 searches the memory 31 for the entry of the key generation apparatus corresponding to the address included in the encrypted message and retrieves it.

[0260] Under the control of the controller unit, a verification unit (not shown) of the first decryption apparatus 30-1 verifies that the schema pair and the policy included in the encrypted message are included in the schema list and the policy list included in the entry obtained from the registration apparatus 50 (step S22a). If this verification fails, the process ends with a decryption processing failure (step S22g).

[0261] When the verification succeeds, an acquisition unit 32 of the first decryption apparatus 30-1 reads the attribute designation information or the predicate designation information corresponding to the user of the first decryption apparatus 30-1 from a storage medium such as the IC card 39 (step S22f). Whether the attribute designation information or the predicate designation information is read depends on the policy included in the encrypted message. More specifically, the read designation information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the encrypted message. When the policy is Cipher_Text_Policy, the acquisition unit 32 reads the attribute designation information from the storage medium. When the policy is Key_Policy, the acquisition unit 32 reads the predicate designation information from the storage medium. The read designation information is hereafter called user information. The acquisition unit 32 of the first decryption apparatus 30-1 may read from the management apparatus 40 the attribute designation information or the predicate designation information corresponding to the user of the first decryption apparatus 30-1, in the same way as in «a user information acquisition process» in the key generation apparatus 20, described later. In the first embodiment of the second aspect, the process of step S22f may be omitted. When the first decryption apparatus 30-1 has the attribute designation information and the predicate designation information corresponding to the user in advance, either the attribute designation information or the predicate designation information serves as user information, according to the policy.

[0262] Next, the verification unit of the first decryption apparatus 30-1 verifies that the decryption apparatus 30 has the decryption key to be used to decrypt the encryption information included in the encryption message (step S22b).

[0263] The first decryption apparatus 30-1 stores a decryption key table in the memory 31. In the decryption key table, as shown in Fig. 15, for example, the identifier of each key generation apparatus is associated with the public parameter, the schema pair, the decryption key target, the predicate designation information, and the decryption key. The verification unit verifies that the decryption apparatus 30 has the decryption key corresponding to the identifier of the key generation apparatus determined from the address included in the encrypted message, to the public parameter, to the schema pair, and to the decryption key target (corresponding to the content of the policy identifying one schema paired with the other schema identified by the policy included in the encrypted message). When the decryption apparatus 30 has the decryption key, the process of step S29 is performed. If the decryption apparatus 30 does not have the decryption key, the process of step S23 is performed.

[0264] The description of «the decryption process» is temporarily halted here and «a key generation process» will be described below.

[0265] If the first decryption apparatus 30-1 does not have the decryption key, the transmitter unit 34 of the first decryption apparatus 30-1 generates, under the control of the controller unit, a key request message that includes the public parameter, the policy, the schema pair, the user information (if any), and the authentication information, all of these items being read from the memory 31. The authentication information includes, for example, the ID of the user and a password. The transmitter unit 34 of the first decryption apparatus 30-1 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message (step S23). The received key request message is stored in a memory 21 of the key generation apparatus 20.

[0266] Under the control of a controller unit, a verification unit (not shown) of the key generation apparatus 20 verifies that the schema pair and the policy included in the key request message are included in the schema list and the policy list included in the entry owned by the key generation apparatus 20 (for example, the entry generated in step S1) and that the public parameter included in the key request message is identical to the public parameter of the key generation apparatus 20 (step S24a). If this verification fails, the process ends with a key generation process failure (step S24g). When the authentication information is included in the key request message, the authentication information is also verified in the process of step S24a. The key generation apparatus 20 stores an authentication table in the memory 21. In the authentication table, as shown in Fig. 16, for example, each user ID is associated with a password. The verification

unit verifies that the user ID and the password included in the key request message are identical to the user ID and the password included in the authentication table. If the verification fails, the process of step S24g is performed.

[0267] When this verification succeeds, the verification unit of the key generation apparatus 20 verifies that the key request message includes the user information (step S24b). When the key request message includes the user information, the process of step S24c is performed. If the key request message does not include the user information, the process of step S25 is performed. When a method is employed in which a key request message always includes user information, the process of step S24b and «a user information acquisition process», described later, are unnecessary.

[0268] The description of «the key generation process» is temporarily halted here and «the user information acquisition process» will be described below.

[0269] The transmitter unit 24 of the key generation apparatus 20 sends a request that includes the policy and the authentication information (if any) included in the key request message to the management apparatus 40, and the management apparatus 40 receives the request (step S25). The received request is stored in a memory of the management apparatus 40.

[0270] The management apparatus 40 stores an authentication table in the memory. In the same way as in the authentication table described above, the user ID is associated with the password in this authentication table (see Fig. 16). A verification unit (not shown) of the management apparatus 40 verifies that the user ID and the password included in the request are identical to the user ID and the password included in the authentication table.

[0271] When this verification succeeds, a searching unit (not shown) of the management apparatus 40 searches a user information table stored in the memory for the attribute designation information or the predicate designation information according to the policy included in the request (step S26). The user information table includes, for example, a first table formed of each user ID, and an attribute name and attribute designation information associated with the user ID, and a second table formed of the user ID and predicate designation information associated with the user ID (see Fig. 17). Whether the attribute designation information or the predicate designation information is read is determined by the policy included in the request. More specifically, the read information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the request. When the policy is Cipher_Text_Policy, the searching unit reads the attribute designation information corresponding to the user ID included in the request from the first table. When the policy is Key_Policy, the searching unit reads the predicate designation information corresponding to the user ID included in the request from the second table. The read designation information is hereafter called user information.

[0272] Under the control of a controller unit, a transmitter unit of the management apparatus 40 sends the user information to the key generation apparatus 20, and the receiver unit of the key generation apparatus 20 receives the user information (step S27). The received user information is stored in the memory 21 of the key generation apparatus 20.

[0273] The description of «the user information acquisition process» ends here, and the description of «the key generation process» will be resumed.

[0274] When the key generation apparatus 20 already has the user information or receives the user information through the user information acquisition process (step S27), a second predicate logic information acquisition unit 23 of the key generation apparatus 20 reads the policy, the schema pair, the public parameter, and the user information from the memory 21, and obtains attribute information (hereafter called second attribute information) or predicate information (second predicate information) from the user information (step S24c). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the first embodiment of the second aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13). The schema is used to extract and arrange necessary attribute values from the input information.

[0275] Next, a key generation unit 25 of the key generation apparatus 20 generates a random number α that is an element of the finite field F_q, based on the public parameter q according to the predicate encryption algorithm, and uses the random number α, the second attribute information $v_{(p)} = (V_{(p)1}, ..., V_{(p)n})$ or the second predicate information $w_{(p)} = (w_{(p)1}, ..., w_{(p)n})$ read from the memory 21, and a private key B* of the key generation apparatus to obtain a decryption key R according to Expression (10) (step S24d). The second predicate information $w_{(p)}$ is used in this example because the input information used in the encryption process is the attribute designation information. When the input information is the predicate designation information, the second attribute information $v_{(p)}$ is used. Therefore, $w_{(p)}$ needs to be replaced with $v_{(p)}$ in Expression (10), described earlier.

[0276] Next, under the control of the controller unit, the transmitter unit 24 of the key generation apparatus 20 sends the decryption key R to the first decryption apparatus 30-1, and the receiver unit of the first decryption apparatus 30-1

receives the decryption key R (step S28). The received decryption key R is stored in the memory 31 of the first decryption apparatus 30-1.

[0277] The description of «the key generation process» ends here, and the description of «the decryption process» will be resumed.

[0278] When the first decryption apparatus 30-1 already has the decryption key or receives the decryption key through the key generation process (step S28), a decryption unit 33 of the first decryption apparatus 30-1 reads the public parameter, the decryption key R, the encryption information C_1, and the ciphertext C_2 (if necessary) from the memory 31, and obtains the common key K and the plaintext M (if necessary) (step S29).

[0279] Details of the process in step S29 will be described below. A first decryption unit 33a reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31, and obtains $e(C_1, R)$ according to the predicate encryption algorithm. As shown in Expression (11), described earlier, the calculation result depends on the result of the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ taken out from the encryption information C_1 and the decryption key R according to bilinearity when the input information is the attribute designation information. When the input information is the predicate designation information, v needs to be replaced with $v_{(p)}$ and $w_{(p)}$ needs to be replaced with w in Expression (11), described earlier. The calculation result depends on the result of the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ taken out from the encryption information C_1 and the decryption key R according to bilinearity. In Expression (11), $e(b_i, b_i^*)$ is defined as shown in Expression (12), described earlier, where δ_{ij} is the Kronecker's delta symbol.

[0280] Therefore, when the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ is zero (or when the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ is zero), the result of calculation in Expression (11), g_T^{ρ}, is obtained. When the result of calculation, g_T^{ρ}, is obtained, the first decryption unit 33a of the first decryption apparatus 30-1 obtains the common key K, which is correct, according to Expression (7), described earlier (step S22c). When the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ is not zero (or when the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ is not zero), the first decryption unit 33a obtains an incorrect value according to Expression (7), described earlier. In this example, it is assumed that the hash function H is common to the system or is included in the public parameter. The encryption information C_1 corresponds to the information p used to generate the common key K in this example. When encryption information C_1 corresponds to the common key K, the result of calculation in Expression (11), described earlier, is the common key K (or incorrect value). In other words, an authorized user of the first decryption apparatus 30-1 has predicate designation information that gives the second predicate information $w_{(p)}$ which makes the canonical inner product with the first attribute information v zero, or attribute designation information that gives the second attribute information $v_{(p)}$ which makes the canonical inner product with the first predicate information w zero.

[0281] Then, a second decryption unit 33b uses the common key K and the ciphertext C_2 to calculate plaintext M according to Expression (13), described earlier (step S22d). A decryption method Dec_K that uses the private key corresponds to the encryption method Enc_K. As described earlier, when the first embodiment of the second aspect is dedicated to the delivery of the common key K, the process of step S22d is omitted. More specifically, even if the first decryption apparatus 30-1 has the function of the second decryption unit 33b, it does not perform the process of step S22d.

[0282] If the result of calculation in Expression (11), described earlier, is an incorrect value, the correct plaintext M cannot be obtained by Expression (13), described earlier.

[0283] The first decryption apparatus 30-1 may store the decryption key R in the decryption key table. In addition, the first decryption apparatus 30-1 may store the common key K in the decryption key table.

[0284] The description of «the first decryption process» ends here.

«Transfer process»

[0285] A transfer unit 37 of the first decryption apparatus 30-1 transfers the encrypted message received from the encryption apparatus 10, to the second decryption apparatus 30-2, and a receiver unit of the second decryption apparatus 30-2 receives the encrypted message (step S30). The decryption apparatus to which the encrypted message is transferred is not limited to the second decryption apparatus (decryption apparatus that does not exchange an encrypted message with the encryption apparatus) and may be another first decryption apparatus (decryption apparatus that exchanges an encrypted message with the encryption apparatus). For the convenience of description, the process of step S30 follows the process of step S29. The process of step S30, however, may be performed anytime after the first decryption apparatus 30-1 receives the encrypted message from the encryption apparatus 10.

[0286] The description of «the transfer process» ends here.

[0287] A second decryption process (that includes a key generation process and, if necessary, a user information acquisition process) performed by the second decryption apparatus 30-2 will be described below. This series of processing is substantially the same as the first decryption process. The second decryption apparatus 30-2 has the same functional

structure as the first decryption apparatus 30-1 except that the transfer unit 37 is not necessarily required. Therefore, the same reference numerals are assigned to the same functional components.

«Second decryption process»

[0288] Under the control of a controller unit, not shown, a transmitter unit 34 of the second decryption apparatus 30-2 sends a search query that includes the address of the key generation apparatus, the address being included in the encrypted message, to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S31). The searching unit of the registration apparatus 50 searches for the entry of the key generation apparatus specified by the address and selects it (step S32). The transmitter unit of the registration apparatus 50 sends the entry of the search result to the second decryption apparatus 30-2, and the receiver unit of the second decryption apparatus 30-2 receives the entry (step S33). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 31 of the second decryption apparatus 30-2.

[0289] When the second decryption apparatus 30-2 has the public parameter, schema list, policy list, and address of each key generation apparatus 20 in advance, the processes of steps S31 to S33 are omitted. In that case, the second decryption apparatus 30-2 searches the memory 31 for the entry of the key generation apparatus corresponding to the address included in the encrypted message and retrieves it.

[0290] Under the control of the controller unit, a verification unit (not shown) of the second decryption apparatus 30-2 verifies that the schema pair and the policy included in the encrypted message are included in the schema list and the policy list included in the entry obtained from the registration apparatus 50 (step S34a). If this verification fails, the process ends with a decryption processing failure (step S34g).

[0291] When the verification succeeds, an acquisition unit 32 of the second decryption apparatus 30-2 reads the attribute designation information or the predicate designation information corresponding to the user of the second decryption apparatus 30-2 from a storage medium such as the IC card 39 (step S34f). Whether the attribute designation information or the predicate designation information is read depends on the policy included in the encrypted message. More specifically, the read designation information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the encrypted message. When the policy is Cipher Text Policy, the acquisition unit 32 reads the attribute designation information from the storage medium. When the policy is Key_Policy, the acquisition unit 32 reads the predicate designation information from the storage medium. The read designation information is hereafter called user information. The acquisition unit 32 of the second decryption apparatus 30-2 may read from the management apparatus 40 the attribute designation information or the predicate designation information corresponding to the user of the second decryption apparatus 30-2, in the same way as in «a user information acquisition process» in the key generation apparatus 20, described later. In the first embodiment of the second aspect, the process of step S34f may be omitted. When the second decryption apparatus 30-2 has the attribute designation information and the predicate designation information corresponding to the user in advance, either the attribute designation information or the predicate designation information serves as user information, according to the policy.

[0292] Next, the verification unit of the second decryption apparatus 30-2 verifies that the decryption apparatus 30 has the decryption key to be used to decrypt the encryption information included in the encryption message (step S34b).

[0293] The second decryption apparatus 30-2 stores a decryption key table in the memory 31. In the decryption key table, as shown in Fig. 15, for example, the identifier of each key generation apparatus is associated with the public parameter, the schema pair, the decryption key target, the predicate designation information, and the decryption key. The verification unit verifies that the decryption apparatus 30 has the decryption key corresponding to the identifier of the key generation apparatus determined from the address included in the encrypted message, to the public parameter, to the schema pair, and to the decryption key target (corresponding to the content of the policy identifying one schema paired with other the schema identified by the policy included in the encrypted message). When the decryption apparatus 30 has the decryption key, the process of step S41 is performed. If the decryption apparatus 30 does not have the decryption key, the process of step S35 is performed.

[0294] The description of «the decryption process» is temporarily halted here and «a key generation process» will be described below.

[0295] If the second decryption apparatus 30-2 does not have the decryption key, the transmitter unit 34 of the second decryption apparatus 30-2 generates, under the control of the controller unit, a key request message that includes the public parameter, the policy, the schema pair, the user information (if any), and the authentication information, all of these items being read from the memory 31. The authentication information includes, for example, the ID of the user and a password. The transmitter unit 34 of the second decryption apparatus 30-2 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message (step S35). The received key request message is stored in a memory

21 of the key generation apparatus 20. This key generation apparatus 20 does not necessarily need to be the key generation apparatus 20 paired with the first decryption apparatus 30-1.

[0296] Under the control of a controller unit, a verification unit (not shown) of the key generation apparatus 20 verifies that the schema pair and the policy included in the key request message are included in the schema list and the policy list included in the entry owned by the key generation apparatus 20 (for example, the entry generated in step S1) and that the public parameter included in the key request message is identical to the public parameter of the key generation apparatus 20 (step S36a). If this verification fails, the process ends with a key generation process failure (step S36g). When the authentication information is included in the key request message, the authentication information is also verified in the process of step S36a. The key generation apparatus 20 stores an authentication table in the memory 21. In the authentication table, as shown in Fig. 16, for example, each user ID is associated with a password. The verification unit verifies that the user ID and the password included in the key request message are identical to the user ID and the password included in the authentication table. If the verification fails, the process of step S36g is performed.

[0297] When this verification succeeds, the verification unit of the key generation apparatus 20 verifies that the key request message includes the user information (step S36b). When the key request message includes the user information, the process of step S36c is performed. If the key request message does not include the user information, the process of step S37 is performed. When a method is employed in which a key request message always includes user information, the process of step S36b and «a user information acquisition process», described later, are unnecessary.

[0298] The description of «the key generation process» is temporarily halted here and «the user information acquisition process» will be described below.

[0299] The transmitter unit 24 of the key generation apparatus 20 sends a request that includes the policy and the authentication information (if any) included in the key request message to the management apparatus 40, and the management apparatus 40 receives the request (step S37). The received request is stored in a memory of the management apparatus 40.

[0300] The management apparatus 40 stores an authentication table in the memory. In the same way as in the authentication table described above, the user ID is associated with the password in this authentication table (see Fig. 16). A verification unit (not shown) of the management apparatus 40 verifies that the user ID and the password included in the request are identical to the user ID and the password included in the authentication table.

[0301] When this verification succeeds, a searching unit (not shown) of the management apparatus 40 searches a user information table stored in the memory for the attribute designation information or the predicate designation information according to the policy included in the request (step S38). The user information table includes, for example, a first table formed of each user ID, and an attribute name and attribute designation information associated with the user ID, and a second table formed of the user ID and predicate designation information associated with the user ID (see Fig. 17). Whether the attribute designation information or the predicate designation information is read is determined by the policy included in the request. More specifically, the read information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the request. When the policy is Cipher_Text_Policy, the searching unit reads the attribute designation information corresponding to the user ID included in the request from the first table. When the policy is Key_Policy, the searching unit reads the predicate designation information corresponding to the user ID included in the request from the second table. The read designation information is hereafter called user information.

[0302] Under the control of a controller unit, a transmitter unit of the management apparatus 40 sends the user information to the key generation apparatus 20, and the receiver unit of the key generation apparatus 20 receives the user information (step S27). The received user information is stored in the memory 21 of the key generation apparatus 20.

[0303] The description of «the user information acquisition process» ends here, and the description of «the key generation process» will be resumed.

[0304] When the key generation apparatus 20 already has the user information or receives the user information through the user information acquisition process (step S39), a second predicate logic information acquisition unit 23 of the key generation apparatus 20 reads the policy, the schema pair, the public parameter, and the user information from the memory 21, and obtains attribute information (hereafter called second attribute information) or predicate information (second predicate information) from the user information (step S36c). In general, the user of the first decryption apparatus 30-1 and the user of the second decryption apparatus 30-2 are different. Therefore, the second attribute information or second predicate information obtained in this process is not necessarily the same as the second attribute information or the second predicate information obtained in the process of step S24c. In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the first embodiment of the second

aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).
The schema is used to extract and arrange necessary attribute values from the input information.

[0305] Next, a key generation unit 25 of the key generation apparatus 20 generates a random number α that is an element of the finite field F_q, based on the public parameter q according to the predicate encryption algorithm, and uses the random number α, the second attribute information $v'_{(p)} = (v'_{(p)1}, ..., v'_{(p)n})$ or the second predicate information $w'_{(p)} = (w'_{(p)1}, ..., w'_{(p)n})$ read from the memory 21, and a private key B* of the key generation apparatus to obtain a decryption key R' according to Expression (14) (step S36d). The second predicate information $w'_{(p)}$ is used in this example because the input information used in the encryption process is the attribute designation information. When the input information is the predicate designation information, the second attribute information $v'_{(p)}$ is used. Therefore, $w'_{(p)}$ needs to be replaced with $v'_{(p)}$ in Expression (14).

$$R' = \varepsilon \sum_{i=1}^{n} w'_{(p)i} b_i^* + b_{n+1}^* \qquad (14)$$

[0306] Next, under the control of the controller unit, the transmitter unit 24 of the key generation apparatus 20 sends the decryption key R' to the second decryption apparatus 30-2, and the receiver unit of the second decryption apparatus 30-2 receives the decryption key R' (step S28). The received decryption key R' is stored in the memory 31 of the second decryption apparatus 30-2.

[0307] The description of «the key generation process» ends here, and the description of «the decryption process» will be resumed.

[0308] When the second decryption apparatus 30-2 already has the decryption key or receives the decryption key through the key generation process (step S40), a decryption unit 33 of the second decryption apparatus 30-2 reads the public parameter, the decryption key R', the encryption information C_1, and the ciphertext C_2 (if necessary) from the memory 31, and obtains the common key K and the plaintext M (if necessary) (step S41).

[0309] Details of the process in step S41 will be described below. The first decryption unit 33a reads the public parameter, the decryption key R', and the encryption information C_1 from the memory 31, and obtains $e(C_1, R)$ according to the predicate encryption algorithm. As shown in Expression (15), the calculation result depends on the result of the canonical inner product of the first attribute information v and the second predicate information $w'_{(p)}$ taken out from the encryption information C_1 and the decryption key R' according to bilinearity when the input information is the attribute designation information. When the input information is the predicate designation information, v needs to be replaced with $v'_{(p)}$ and $w'_{(p)}$ needs to be replaced with w in Expression (15). The calculation result depends on the result of the canonical inner product of the first predicate information w and the second attribute information $v'_{(p)}$ taken out from the encryption information C_1 and the decryption key R' according to bilinearity. In Expression (15), $e(b_i, b_i^*)$ is defined as shown in Expression (12), described earlier.

$$\begin{aligned} e(C_1, R') &= e(r\sum_{i=1}^{n} v_i b_i, R') \cdot e(\rho b_{n+1}, R') \\ &= \prod_{i=1}^{n} e(b_i, b_i^*)^{r\alpha v_i w'_{(p)i}} \cdot e(b_{n+1}, b_{n+1}^*)^{\rho} \\ &= g_T{}^{r\alpha \sum_{i=1}^{n} v_i w'_{(p)i}} \cdot g_T{}^{\rho} \\ &= g_T{}^{r\alpha v \cdot w'_{(p)}} \cdot g_T{}^{\rho} \end{aligned} \qquad (15)$$

[0310] Therefore, when the canonical inner product of the first attribute information v and the second predicate information $w'_{(p)}$ is zero (or when the canonical inner product of the first predicate information w and the second attribute

information $v'_{(p)}$ is zero), the result of calculation in Expression (15), g_T^{ρ}, is obtained. When the result of calculation, g_T^{ρ}, is obtained, the first decryption unit 33a of the second decryption apparatus 30-2 obtains the common key K, which is correct, according to Expression (7), described earlier (step S34c). When the canonical inner product of the first attribute information v and the second predicate information $w'_{(p)}$ is not zero (or when the canonical inner product of the first predicate information w and the second attribute information $v'_{(p)}$ is not zero), the first decryption unit 33a obtains an incorrect value according to Expression (7), described earlier. In this example, it is assumed that the hash function H is common to the system or is included in the public parameter. The encryption information C_1 corresponds to the information p used to generate the common key K in this example. When encryption information C_1 corresponds to the common key K, the result of calculation in Expression (15) is the common key K (or incorrect value). In other words, an authorized user of the second decryption apparatus 30-2 has predicate designation information that gives the second predicate information $w'_{(p)}$ which makes the canonical inner product with the first attribute information v zero, or attribute designation information that gives the second attribute information $v'_{(p)}$ which makes the canonical inner product with the first predicate information w zero.

[0311] Then, the second decryption unit 33b uses the common key K and the ciphertext C_2 to calculate plaintext M according to Expression (13), described earlier (step S34d). A decryption method Dec_K that uses the private key corresponds to the encryption method Enc_K. As described earlier, when the first embodiment of the second aspect is dedicated to the delivery of the common key K, the process of step S34d is omitted. More specifically, even if the second decryption apparatus 30-2 has the function of the second decryption unit 33b, it does not perform the process of step S34d.

[0312] If the result of calculation in Expression (15) is an incorrect value, the correct plaintext M cannot be obtained by Expression (13), described earlier.

[0313] The second decryption apparatus 30-2 may store the decryption key R' in the decryption key table. In addition, the second decryption apparatus 30-2 may store the common key K in the decryption key table.

[0314] The description of «the second decryption process» ends here.

[0315] When the second decryption apparatus 30-2 has a transfer unit 37, the second decryption apparatus 30-2 may transfer the encrypted message received from the first decryption apparatus 30-1, to another second decryption apparatus (decryption apparatus that does not exchange an encrypted message with the encryption apparatus) or to the first decryption apparatus (decryption apparatus that exchanges an encrypted message with the encryption apparatus). This transfer process may be performed anytime after the second decryption apparatus 30-2 receives the encrypted message from the first decryption apparatus 30-1.

(Second embodiment according to second aspect)

[0316] A second embodiment of the second aspect differs from the first embodiment of the second aspect in that the first decryption apparatus 30-1 and the second decryption apparatus 30-2 generate the second attribute information or the second predicate information. Because of this difference, the second embodiment of the second aspect differs in several points from the first embodiment of the second aspect. A description of commonalities between the first and second embodiments of the second aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the second aspect will be made with reference to Figs. 42 to 48.

[0317] The processes of steps S1 to S22 are the same as those in the first embodiment of the second aspect.

[0318] When the decryption key is not possessed in the process of step S22b, a second predicate logic information acquisition unit 35 of the first decryption apparatus 30-1 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S23g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the second embodiment of the second aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0319] After the process of step S23g, the process of step 23 is performed. In this process, the transmitter unit 34 of the first decryption apparatus 30-1 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the first decryption apparatus 30-1 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0320] When the verification succeeds in the process of step S24a, the process of step S24d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the first decryption apparatus 30-1, the function and the process for generating the information are unnecessary, unlike in the first embodiment of the second aspect.

[0321] The processes of steps S28 to S34a, to be performed after the process of step S24d, are the same as those in the first embodiment of the second aspect.

[0322] When the decryption key is not possessed in the process of step S34b, a second predicate logic information acquisition unit 35 of the second decryption apparatus 30-2 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S35g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the second embodiment of the second aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0323] After the process of step S35g, the process of step 35 is performed. In this process, the transmitter unit 34 of the second decryption apparatus 30-2 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the second decryption apparatus 30-2 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0324] When the verification succeeds in the process of step S36a, the process of step S36d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the second decryption apparatus 30-2, the function and the process for generating the information are unnecessary, unlike in the first embodiment of the second aspect.

[0325] The processes of steps S40 and S41, following the process of step S36d, are the same as those in the first embodiment of the second aspect.

(Third embodiment according to second aspect)

[0326] A third embodiment of the second aspect differs from the first embodiment of the second aspect in that the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key and included in the public parameter the plaintext M read from the memory 11 to obtain encryption information C_1. In other words, the predicate encryption algorithm disclosed in Non-patent literature 2, for example, is used in the third embodiment of the second aspect. Because of this difference, the third embodiment of the second aspect differs in several points from the first embodiment of the second aspect. A description of commonalities between the first and third embodiments of the second aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the second aspect will be made with reference to Figs. 49 to 54.

[0327] The processes of steps S1 to S17a are the same as those in the first embodiment of the second aspect. The public parameter and some other information are required by the predicate encryption algorithm of the third embodiment of the second aspect. For specific information required, see Non-patent literature 2, described above, for example.

[0328] In the process of step S17b1, following the process of step S17a, the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1 according to the predicate encryption algorithm (step S17b1).

[0329] After the process of step S17b1, the process of step 17d is performed. In this process, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1, and the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 31, under the control of the controller unit (step S 17d).

[0330] The processes of steps S18 to S28, following the process of step S17d, are the same as those in the first embodiment of the second aspect.

[0331] In the process of step S22c1, following the process of step S28, the decryption unit 33 of the first decryption apparatus 30-1 reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31 to calculate plaintext M according to the predicate encryption algorithm (step S22c1).

[0332] The processes of steps S30 to S40, following the process of step S22c1, are the same as those in the first embodiment of the second aspect.

[0333] In the process of step S34c1, following the process of step S40, the decryption unit 33 of the second decryption apparatus 30-2 reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31 to calculate plaintext M according to the predicate encryption algorithm (step S34c1).

(Fourth embodiment according to second aspect)

[0334] A fourth embodiment of the second aspect corresponds to a combination of the second embodiment of the second aspect and the third embodiment of the second aspect. The fourth embodiment of the second aspect differs from the first embodiment of the second aspect in that (1) the first decryption apparatus 30-1 and the second decryption apparatus 30-2 generate the second attribute information or the second predicate information, and (2) the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1. Because of these differences, the fourth embodiment of the second aspect differs in several points from the first embodiment of the second aspect. A description of commonalities between the first and fourth embodiments of the second aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the second aspect will be made with reference to Figs. 55 to 58.

[0335] The processes of steps S1 to S17a are the same as those in the first embodiment of the second aspect. The public parameter and some other information are required by the predicate encryption algorithm of the fourth embodiment of the second aspect. For specific information required, see Non-patent literature 2, described above, for example.

[0336] In the process of step S17b1, following the process of step S17a, the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the plaintext M read from the memory 11, to obtain encryption information C_1 according to the predicate encryption algorithm (step S17b1).

[0337] After the process of step S17b1, the process of step 17d is performed. In this process, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1, and the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 31, under the control of the controller unit (step S 17d).

[0338] The processes of steps S18 to S22b, following the process of step S17d, are the same as those in the first embodiment of the second aspect.

[0339] When the decryption key is not possessed in the process of step S22b, the second predicate logic information acquisition unit 35 of the first decryption apparatus 30-1 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S23g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the fourth embodiment of the second aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0340] After the process of step S23g, the process of step 23 is performed. In this process, the transmitter unit 34 of the first decryption apparatus 30-1 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the first decryption apparatus 30-1 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0341] When the verification succeeds in the process of step S24a, the process of step S24d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the first decryption apparatus 30-1, the function and the process for generating the information are unnecessary.

[0342] The process of step S28, following the process of step S24d, is the same as that in the first embodiment of the second aspect.

[0343] In the process of step S22c1, following the process of step S28, the decryption unit 33 of the first decryption apparatus 30-1 reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31 to calculate plaintext M according to the predicate encryption algorithm (step S22c1).

[0344] The processes of steps S30 to S34, following the process of step S22c1, are the same as those in the first embodiment of the second aspect.

[0345] When the decryption key is not possessed in the process of step S34b, the second predicate logic information acquisition unit 35 of the second decryption apparatus 30-2 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S35g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the fourth embodiment of the second aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0346] After the process of step S35g, the process of step 35 is performed. In this process, the transmitter unit 34 of the second decryption apparatus 30-2 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the second decryption apparatus 30-2 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0347] When verification succeeds in the process of step S36a, the process of step S36d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the second decryption apparatus 30-2, the function and the process for generating the information are unnecessary, unlike in the first embodiment of the second aspect.

[0348] The process of step S40, following the process of step S36d, is the same as that in the first embodiment of the second aspect.

[0349] In the process of step S34c1, following the process of step S40, the decryption unit 33 of the second decryption apparatus 30-2 reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31 to calculate plaintext M according to the predicate encryption algorithm (step S34c1).

[0350] The above described embodiments of the second aspect are implemented, for example, as email systems or instant message systems. Fig. 59 shows the structure of data exchanged. The basic format of the entire message conforms, for example, to S/MIME (Secure Multipurpose Internet Mail Extensions). An appropriate data structure is given to data from the start position marker of an encrypted message to the end position marker of the encrypted message in XML (the extensible Markup Language) or other some language.

[0351] A series of data concerning the predicate encryption is disposed from the start position marker of an encrypted message to the end position marker of the encrypted message.

[0352] An algorithm identifier block specifies information that identifies the predicate encryption algorithm used to encrypt the private key and the private key encryption algorithm used to encrypt the message payload. An identifier indicating the algorithm or the version of an algorithm (for example, PE/Version X + Camellia (Camellia is a registered trademark)) can be specified.

[0353] A digital signature block specifies the digital signature. A known signature algorithm can be used. This item can be omitted depending on the application.

[0354] A public parameter information block specifies information that identifies the public parameter used. An identifier that identifies the public parameter or the data of the public parameter can be specified.

[0355] A policy field specifies an identifier that identifies the policy used.

[0356] A schema field specifies an identifier that identifies the schema used or the data of the schema.

[0357] An encryption information field specifies the data (encryption information) obtained by encrypting, with the predicate encryption, the private key used to encrypt the message payload (plaintext).

[0358] An ciphertext field specifies the data (ciphertext) obtained by encrypting the message payload (plaintext).

[0359] An attribute field and a predicate field specify letter string representations that indicate the attribute and the predicate used for encryption, corresponding to the policy field, respectively. These items can be omitted according to the application.

[0360] An attachment field can include an attachment file encrypted with RSA, for example. This item can be omitted according to the application.

[0361] In secure communication for instant messaging, for example, it is not necessary to resend the encryption information obtained by encrypting the private key. In usual instant messaging, when an appropriate private key is obtained in the first instant message, the receiver may store the private key to decrypt subsequent instant messages. In that case, the sender just sends ciphertext to the receiver but may not send the public parameter, the policy, the

schema, or the encryption information in the subsequent instant messages. In the same way, when the encryption algorithm used is not changed, the encryption algorithm identifier may be omitted in the subsequent instant messages.

[0362] Predicate encryption does not depend on information based on the receiver, in encryption. Therefore, the sender (sending apparatus) can send an encrypted message to an unknown receiver (receiving apparatus). In other words, the sender performs encryption just once even if there are a plurality of receivers (receiving apparatuses) (in the public key cryptosystem, encryption needs to be performed N times). Therefore, the sender (sending apparatus) can send an encrypted message to a plurality of receivers at a low cost.

[0363] The receiver (receiving apparatus) can transfer the encrypted message received from the encryption apparatus to a third party (apparatus). In the public key cryptosystem, the receiver (receiving apparatus) needs to decrypt the encrypted message, encrypt the original message with the public key of the third party (apparatus), and send the encrypted message, causing a high processing cost. In the above-described embodiments, since the encrypted message received from the encryption apparatus can be transferred to the third party (apparatus) without any processing, the encrypted message is transferred at a low processing cost.

[0364] Embodiments according to a third aspect of the present invention, which relate to a cryptographic communication technology that can operate flexibly, that is based on predicate encryption, and that allows content (encrypted content) encrypted with the predicate encryption to be distributed will be described next while attention is being paid to the cryptographic communication technology of the first aspect, described above. In the cryptographic communication technology of the third aspect, content (encrypted content) encrypted with predicate encryption is stored in a content server, and the encrypted content is distributed to a decryption apparatus upon request.

[0365] The description of the cryptographic communication technology of the third aspect and the description of the cryptographic communication technology of the first aspect have many substantial commonalities, but, to avoid referring to the description of the cryptographic communication technology of the first aspect, the cryptographic communication technology of the third aspect will be described below with overlapping explanations and figures being included as much as possible. Therefore, in both descriptions, identical expression numbers, identical reference numerals assigned to function blocks, and identical reference numerals assigned to steps are used. Because the contexts are different, there should be no risk of confusion.

(First embodiment according to third aspect)

[0366] A first embodiment according to the third aspect of the present invention will be described below with reference to Fig. 60 to Fig. 71.

[0367] As shown in Fig. 60, a cryptographic system 1 according to the third aspect includes a plurality of client apparatuses 10 and 30, one or a plurality of key generation apparatuses 20, one or a plurality of content servers 60, one or a plurality of user information management apparatuses 40 (hereafter each called a management apparatus), conversion rule information pair management apparatuses 50 (hereafter each called a registration apparatus), one or a plurality of maintenance apparatuses 80, and one or a plurality of authentication apparatuses 90. These apparatuses can communicate with each other through a communication network 5, such as the Internet.

[0368] The client apparatuses function as encryption apparatuses for encrypting content to generate encrypted content or decryption apparatuses for decrypting the encrypted content, based on their processing functions. Depending on their functions, the client apparatuses are called encryption apparatuses 10 or decryption apparatuses 30. The cryptographic system 1 of the third aspect may include client apparatuses that function only as encryption apparatuses and/or client apparatuses that function only as decryption apparatuses.

[0369] In the cryptographic system 1 of the third aspect, encryption and decryption are performed using predicate encryption. In the third aspect of the present invention, the predicate encryption algorithm to be used is not limited, and the predicate encryption algorithm disclosed in Non-patent literature 2, for example, may be used. In the first embodiment of the third aspect, a predicate encryption algorithm of KEM (the key encapsulation mechanism) type will be used.

[0370] A cryptographic communication method used in the cryptographic system 1 will be described with reference to Figs. 61, 62, 63, 64, 66, 69, and 71. See Figs. 65, 67, 68, and 70 for the functional structure of each apparatus.

«Preparation process»

[0371] The entire description of «the preparation process» in the first embodiment of the first aspect according to the present invention is incorporated here and a description of «the preparation process» is omitted. See Fig. 61 for the preparation process, Figs. 11 to 13 for schema pairs, and Fig. 14 for policy lists. The description of the preparation process ends here.

«Encryption process»

[0372] Under the control of a controller unit, not shown, a transmitter unit 14 of the encryption apparatus 10 sends a search query to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S14). The searching unit of the registration apparatus 50 searches some or all of the entries registered in the storage unit of the registration apparatus 50 and chooses one entry (step S15). The transmitter unit of the registration apparatus 50 sends the entry to the encryption apparatus 10, and a receiver unit of the encryption apparatus 10 receives the entry (step S16). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 11 of the encryption apparatus 10.

[0373] When the encryption apparatus 10 has the public parameter, schema list, policy list, and address of each key generation apparatus 20 in advance, the processes of steps S 14 to S16 are omitted. It should be noted that the cryptographic system 1 may have no registration apparatus 50.

[0374] A first predicate logic information acquisition unit 12 of the encryption apparatus 10 reads the input information, the policy, and the schemas from the memory 11 and obtains attribute information (hereafter called first attribute information) and predicate information (hereafter called first predicate information) (step S17a). Details of this process will be described below with reference to Figs. 12 and 13.

[0375] When the schema list has a plurality of schema pairs, one schema pair is selected based on the usage or the like. The user of the encryption apparatus 10 may select a schema pair and input designation information thereof. Alternatively, the first predicate logic information acquisition unit 12 may select a schema pair according to a predetermined rule.

[0376] According to whether the input information is attribute designation information or predicate designation information, one of the schemas is selected together with the policy. The user of the encryption apparatus 10 may select the policy and one of the schemas and input designation information thereof. Alternatively, the first predicate logic information acquisition unit 12 may select the policy and one of the schemas according to a predetermined rule. When only one type of policy is prepared in the key generation apparatus 20, one schema of the schema pair is selected according to the policy. If the selected schema does not correspond to the type of the input information, a schema pair needs to be selected again from the schema list or an entry needs to be provided by the registration apparatus 50 again.

[0377] The input information may be information inputted by the user of the encryption apparatus 10 or information acquired by an acquisition unit (not shown) of the encryption apparatus 10 from a storage medium such as an IC card 39.

[0378] Then, the first predicate logic information acquisition unit 12 uses the schema selected from the schema pair according to the policy to obtain the first attribute information or the first predicate information from the input information. When the policy is Key_Policy and the selected schema is an attribute schema, the first attribute information is obtained. When the policy is Cipher_Text_Policy and the selected schema is a predicate schema, the first predicate information is obtained. The first attribute information and the first predicate information are vector information having elements of the finite field F_q as components in the first embodiment according to the third aspect (see Figs. 11 to 13). The schema is used to extract or arrange necessary attribute values from the input information.

[0379] Next, an encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, an orthogonal basis B (substantial public key) included in the public parameter read from the memory 11, and content M to obtain a common key K, encryption information C_1, and ciphertext C_2 (steps S 17b and S17c). Details of these processes will be described below.

[0380] A first encryption unit 13a generates random numbers r and p which are elements of the finite field Fq according to the predicate encryption algorithm, specifies the common key K as shown by Expression (7), described earlier, and obtains the encryption information C_1 according to Expression (8) (step S17b), where H indicates, for example, a hash function. In this example, the first attribute information v is used. To use the first predicate information, v needs to be replaced with w in Expression (8), described earlier. In this example, the encryption information C_1 corresponds to p used to generate the common key K. The encryption information C_1 may correspond to the common key K.

[0381] Next, the second encryption unit 13b uses the common key K and the content M to obtain the ciphertext C_2 according to Expression (9), described earlier (step S17c). An encryption method Enc_k that uses the private key can be a known method. For example, it may be the method disclosed in Non-patent literature 1.

[0382] Next, under the control of the controller unit, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encryption information C_1 and the encrypted content C_2, together with the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 11 (step S17d). The transmitter unit 14 of the encryption apparatus 10 then sends the encrypted message to the content server 60, and a receiver unit of the content server 60 receives the encrypted message (step S18). The encrypted content is uploaded by a known method such as FTP (file transfer protocol) or WebDAV (distributed authoring and versioning protocol for the WWW).

[0383] The description of «the encryption process» ends here.

«Content delivery process»

[0384] Under the control of a controller unit, the content server 60 stores, in a memory 61 thereof, the encrypted message sent from each encryption apparatus 10. With this, the encryption information and the encrypted content included in the encrypted message are registered in the content server 60. The encrypted content registered in the content server 60 is made public, for example, on a web page.

[0385] The web page is displayed on a display unit, now shown, of the decryption apparatus 30 by a browser unit 38 of the decryption apparatus 30 according to the Internet protocol. The user of the decryption apparatus 30 performs an input operation to select a desired encrypted content. Based on the user input information, the browser unit 38 of the decryption apparatus 30 sends an acquisition request for acquiring the selected encrypted content from the content server 60, to a decryption unit 33 (hereafter called a relay unit) of the decryption apparatus 30 (step S19). Then, the relay unit 33 of the decryption apparatus 30 sends this acquisition request to the content server 60, and a receiver unit of the content server 60 receives the acquisition request (step S20). In this way, the browser unit 38 and the content server 60 performs exchanges through the relay unit 33 according to, for example, HTTP (hyper text transfer protocol) (the proxy setting of a WWW browser may be used). A searching unit 62 of the content server 60 searches for the encrypted message that includes the encrypted content specified in the acquisition request and selects it (step S21). A transmitter unit 64 of the content server 60 sends the encrypted message to the decryption apparatus 30 under the control of the searching unit 62, and a receiver unit of the decryption apparatus receives the encrypted message (step S22).

[0386] The description of «the content delivery process» ends here.

«Decryption process»

[0387] Under the control of a controller unit, not shown, a transmitter unit 34 of the decryption apparatus 30 sends a search query that includes the address of the key generation apparatus, the address being included in the encrypted message, to the registration apparatus 50, and the receiving unit of the registration apparatus 50 receives the search query (step S23). The searching unit of the registration apparatus 50 searches for the entry of the key generation apparatus specified by the address and selects it (step S24). The transmitter unit of the registration apparatus 50 sends the entry of the search result to the decryption apparatus 30, and the receiver unit of the decryption apparatus 30 receives the entry (step S25). This entry includes the address of the key generation apparatus, the public parameter of the key generation apparatus, the policy list that can be used by the key generation apparatus, and the schema list that can be used by the key generation apparatus. The received entry is stored in a memory 31 of the decryption apparatus 30.

[0388] When the decryption apparatus 30 has the public parameter, schema list, policy list, and address of each key generation apparatus 20 in advance, the processes of steps S 19 to S21 are omitted. In that case, the decryption apparatus 30 searches the memory 31 for the entry of the key generation apparatus corresponding to the address included in the encrypted message and retrieves it.

[0389] Under the control of the controller unit, a verification unit (not shown) of the decryption apparatus 30 verifies that the schema pair and the policy included in the encrypted message are included in the schema list and the policy list included in the entry obtained from the registration apparatus 50 (step S26a). If this verification fails, the process ends with a decryption processing failure (step S26g).

[0390] When the verification succeeds, an acquisition unit 32 of the decryption apparatus 30 reads the attribute designation information or the predicate designation information corresponding to the user of the decryption apparatus 30 from a storage medium such as the IC card 39 (step S26f). Whether the attribute designation information or the predicate designation information is read depends on the policy included in the encrypted message. More specifically, the read designation information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the encrypted message. When the policy is Cipher_Text_Policy, the acquisition unit 32 reads the attribute designation information from the storage medium. When the policy is Key_Policy, the acquisition unit 32 reads the predicate designation information from the storage medium. The read designation information is hereafter called user information. The acquisition unit 32 of the decryption apparatus 30 may read from the management apparatus 40 the attribute designation information or the predicate designation information corresponding to the user of the decryption apparatus 30, in the same way as in «a user information acquisition process» in the key generation apparatus 20, described later. In the first embodiment of the third aspect, the process of step S26f may be omitted. When the decryption apparatus 30 has the attribute designation information and the predicate designation information corresponding to the user in advance, either the attribute designation information or the predicate designation information serves as user information, according to the policy.

[0391] Next, the verification unit of the decryption apparatus 30 verifies that the decryption apparatus 30 has the decryption key to be used to decrypt the encryption information included in the encryption message (step S26b).

[0392] The decryption apparatus 30 stores a decryption key table in the memory 31. In the decryption key table, as

shown in Fig. 15, for example, the identifier of each key generation apparatus is associated with the public parameter, the schema pair, the decryption key target, the predicate designation information, and the decryption key. The verification unit verifies that the decryption apparatus 30 has the decryption key corresponding to the identifier of the key generation apparatus determined from the address included in the encrypted message, to the public parameter, to the schema pair, and to the decryption key target (corresponding to the content of the policy identifying one schema paired with other the schema identified by the policy included in the encrypted message). When the decryption apparatus 30 has the decryption key, the process of step S33 is performed. If the decryption apparatus 30 does not have the decryption key, the process of step S27 is performed.

[0393] The description of «the decryption process» is temporarily halted here and «a key generation process» will be described below.

[0394] If the decryption apparatus 30 does not have the decryption key, the transmitter unit 34 of the decryption apparatus 30 generates, under the control of the controller unit, a key request message that includes the public parameter, the policy, the schema pair, the user information (if any), and the authentication information, all of these items being read from the memory 31. The authentication information includes, for example, the ID of the user and a password. The transmitter unit 34 of the decryption apparatus 30 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message (step S27). The received key request message is stored in a memory 21 of the key generation apparatus 20.

[0395] Under the control of a controller unit, a verification unit (not shown) of the key generation apparatus 20 verifies that the schema pair and the policy included in the key request message are included in the schema list and the policy list included in the entry owned by the key generation apparatus 20 (for example, the entry generated in step S1) and that the public parameter included in the key request message is identical to the public parameter of the key generation apparatus 20 (step S28a). If this verification fails, the process ends with a key generation process failure (step S28g). When the authentication information is included in the key request message, the authentication information is also verified in the process of step S28a. The key generation apparatus 20 stores an authentication table in the memory 21. In the authentication table, as shown in Fig. 16, for example, each user ID is associated with a password. The verification unit verifies that the user ID and the password included in the key request message are identical to the user ID and the password included in the authentication table. If the verification fails, the process of step S28g is performed.

[0396] When this verification succeeds, the verification unit of the key generation apparatus 20 verifies that the key request message includes the user information (step S28b). When the key request message includes the user information, the process of step S28c is performed. If the key request message does not include the user information, the process of step S29 is performed. When a method is employed in which a key request message always includes user information, the process of step S28b and «a user information acquisition process», described later, are unnecessary.

[0397] The description of «the key generation process» is temporarily halted here and «the user information acquisition process» will be described below.

[0398] The transmitter unit 24 of the key generation apparatus 20 sends a request that includes the policy and the authentication information (if any) included in the key request message to the management apparatus 40, and the management apparatus 40 receives the request (step S29). The received request is stored in a memory of the management apparatus 40.

[0399] The management apparatus 40 stores an authentication table in the memory. In the same way as in the authentication table described above, the user ID is associated with the password in this authentication table (see Fig. 16). A verification unit (not shown) of the management apparatus 40 verifies that the user ID and the password included in the request are identical to the user ID and the password included in the authentication table.

[0400] When this verification succeeds, a searching unit (not shown) of the management apparatus 40 searches a user information table stored in the memory for the attribute designation information or the predicate designation information according to the policy included in the request (step S30). The user information table includes, for example, a first table formed of each user ID, and an attribute name and attribute designation information associated with the user ID, and a second table formed of the user ID and predicate designation information associated with the user ID (see Fig. 17). Whether the attribute designation information or the predicate designation information is read is determined by the policy included in the request. More specifically, the read information corresponds to the content of the policy identifying one schema paired with the other schema identified by the policy included in the request. When the policy is Cipher_Text_Policy, the searching unit reads the attribute designation information corresponding to the user ID included in the request from the first table. When the policy is Key_Policy, the searching unit reads the predicate designation information corresponding to the user ID included in the request from the second table. The read designation information is hereafter called user information.

[0401] Under the control of a controller unit, a transmitter unit of the management apparatus 40 sends the user information to the key generation apparatus 20, and the receiver unit of the key generation apparatus 20 receives the user information (step S31). The received user information is stored in the memory 21 of the key generation apparatus 20.

[0402] The description of «the user information acquisition process» ends here, and the description of «the key generation process» will be resumed.

[0403] When the key generation apparatus 20 already has the user information or receives the user information through the user information acquisition process (step S31), a second predicate logic information acquisition unit 23 of the key generation apparatus 20 reads the policy, the schema pair, the public parameter, and the user information from the memory 21, and obtains attribute information (hereafter called second attribute information) or predicate information (second predicate information) from the user information (step S28c). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the first embodiment of the third aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13). The schema is used to extract and arrange necessary attribute values from the input information.

[0404] Next, a key generation unit 25 of the key generation apparatus 20 generates a random number α that is an element of the finite field F_q, based on the public parameter q according to the predicate encryption algorithm, and uses the random number α, the second attribute information $v_{(p)} = (V_{(p)1}, ..., V_{(p)n})$ or the second predicate information $w_{(p)} = (w_{(p)1}, ..., w_{(p)n})$ read from the memory 21, and a private key B* of the key generation apparatus to obtain a decryption key R according to Expression (10), described earlier (step S28d). The second predicate information $w_{(p)}$ is used in this example because the input information used in the encryption process is the attribute designation information. When the input information is the predicate designation information, the second attribute information $v_{(p)}$ is used. Therefore, $w_{(p)}$ needs to be replaced with $v_{(p)}$ in Expression (10), described earlier.

[0405] Next, under the control of the controller unit, the transmitter unit 24 of the key generation apparatus 20 sends the decryption key R to the decryption apparatus 30, and the receiver unit of the decryption apparatus 30 receives the decryption key R (step S32). The received decryption key R is stored in the memory 31 of the decryption apparatus 30.

[0406] The description of <<the key generation process<< ends here, and the description of «the decryption process» will be resumed.

[0407] When the decryption apparatus 30 already has the decryption key or receives the decryption key through the key generation process (step S32), the relay unit 33 of the decryption apparatus 30 reads the public parameter, the decryption key R, the encryption information C_1, and the encrypted content C_2 (if necessary) from the memory 31, and obtains the common key K and the content M (if necessary) (step S33).

[0408] Details of the process in step S33 will be described below. The relay unit 33 includes a first decryption unit 33a and a second decryption unit 33b for decryption.

[0409] The first decryption unit 33a reads the public parameter, the decryption key R, and the encryption information C_1 from the memory 31, and obtains $e(C_1, R)$ according to the predicate encryption algorithm. As shown in Expression (11), described earlier, the calculation result depends on the result of the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ taken out from the encryption information C_1 and the decryption key R according to bilinearity when the input information is the attribute designation information. When the input information is the predicate designation information, v needs to be replaced with $v_{(p)}$ and $w_{(p)}$ needs to be replaced with w in Expression (11), described earlier. The calculation result depends on the result of the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ taken out from the encryption information C_1 and the decryption key R according to bilinearity. In Expression (11), $e(b_i, b_i^*)$ is defined as shown in Expression (12), described earlier, where δ_{ij} is the Kronecker's delta symbol.

[0410] Therefore, when the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ is zero (or when the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ is zero), the result of calculation in Expression (11), g_T^{ρ}, is obtained. When the result of calculation, g_T^{ρ}, is obtained, the first decryption unit 33a of the decryption apparatus 30 obtains the common key K, which is correct, according to Expression (7), described earlier (step S26c). When the canonical inner product of the first attribute information v and the second predicate information $w_{(p)}$ is not zero (or when the canonical inner product of the first predicate information w and the second attribute information $v_{(p)}$ is not zero), the first decryption unit 33a obtains an incorrect value according to Expression (7), described earlier. In this example, it is assumed that the hash function H is common to the system or is included in the public parameter. The encryption information C_1 corresponds to the information p used to generate the common key K in this example. When encryption information C_1 corresponds to the common key K, the result of calculation in Expression (11), described earlier, is the common key K (or incorrect value). In other words, an authorized user of the decryption apparatus 30 has predicate designation information that gives the second predicate information $w_{(p)}$ which makes the canonical inner product with the first attribute information v zero, or attribute designation

information that gives the second attribute information $v_{(p)}$ which makes the canonical inner product with the first predicate information w zero.

[0411] Then, a second decryption unit 33b uses the common key K and the encrypted content C_2 to calculate content M according to Expression (13), described earlier (step S26d). A decryption method Dec_K that uses the private key corresponds to the encryption method Enc_K.

[0412] If the result of calculation in Expression (11), described earlier, is an incorrect value, the correct plaintext M cannot be obtained by Expression (13), described earlier.

[0413] The decryption apparatus 30 may store the decryption key R in the decryption key table. In addition, the decryption apparatus 30 may store the common key K in the decryption key table.

[0414] The content M, obtained by decrypting the encrypted content, is sent from the relay unit 33 to the browser unit 38 (step S34), and the browser unit 38 displays the content M on a display unit of the decryption apparatus 30 (step S35).

[0415] The description of «the decryption process» ends here.

(Second embodiment according to third aspect)

[0416] A second embodiment of the third aspect differs from the first embodiment of the third aspect in that the decryption apparatus 30 generates the second attribute information or the second predicate information. Because of this difference, the second embodiment of the third aspect differs in several points from the first embodiment of the third aspect. A description of commonalities between the first and second embodiments of the third aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the third aspect will be made with reference to Figs. 72 to 75.

[0417] The processes of steps S1 to S26b are the same as those in the first embodiment of the third aspect.
When the decryption key is not possessed in the process of step S26b, a second predicate logic information acquisition unit 35 of the decryption apparatus 30 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S27g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the second embodiment of the third aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0418] After the process of step S27g, the process of step 27 is performed. In this process, the transmitter unit 34 of the decryption apparatus 30 generates a key request message that includes the public parameter, the policy, the schema pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the decryption apparatus 30 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0419] When the verification succeeds in the process of step S28a, the process of step S28d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the decryption apparatus 30, the function and the process for generating the information are unnecessary, unlike in the first embodiment of the third aspect.

[0420] The processes of steps S32 to S35, to be performed after the process of step S28d, are the same as those in the first embodiment of the third aspect.

(Third embodiment according to third aspect)

[0421] A third embodiment of the third aspect differs from the first embodiment of the third aspect in that the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the content M read from the memory 11, to obtain encrypted content C_1. In other words, the predicate encryption algorithm disclosed in Non-patent literature 2, for example, is used in the third embodiment of the third aspect. Because of this difference, the third embodiment of the third aspect differs in several points from the first embodiment of the third aspect. A description of commonalities between the first and third embodiments of the third aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the third aspect will be made with reference to Figs. 76 to 79.

[0422] The processes of steps S1 to S17a are the same as those in the first embodiment of the third aspect. The public parameter and some other information are required by the predicate encryption algorithm of the third embodiment of the third aspect. For specific information required, see Non-patent literature 2, described above, for example.

[0423] In the process of step S17b1, following the process of step S17a, the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the content M read from the memory 11, to obtain encrypted content C_1 according to the predicate encryption algorithm (step S17b1).

[0424] After the process of step S17b1, the process of step 17d is performed. In this process, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encrypted content C_1, and the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 31, under the control of the controller unit (step S 17d).

[0425] The processes of steps S18 to S32, following the process of step S17d, are the same as those in the first embodiment of the third aspect.

[0426] In the process of step S26c1, following the process of step S32, a decryption unit 33c included in the relay unit 33 of the decryption apparatus 30 reads the public parameter, the decryption key R, and the encrypted content C_1 from the memory 31 to calculate content M according to the predicate encryption algorithm (step S26c1).

[0427] The processes of steps S34 and S35, following the process of step S26c1, are the same as those in the first embodiment of the third aspect.

(Fourth embodiment according to third aspect)

[0428] A fourth embodiment of the third aspect corresponds to a combination of the second embodiment of the third aspect and the third embodiment of the third aspect. The fourth embodiment of the third aspect differs from the first embodiment of the third aspect in that (1) the decryption apparatus 30 generates the second attribute information or the second predicate information, and (2) the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the content M read from the memory 11, to obtain encrypted content C_1. Because of these differences, the fourth embodiment of the third aspect differs in several points from the first embodiment of the third aspect. A description of commonalities between the first and fourth embodiments of the third aspect is omitted (the same reference numerals are assigned to the same components), and a description of the differences from the first embodiment of the third aspect will be made with reference to Figs. 80 and 81.

[0429] The processes of steps S1 to S17a are the same as those in the first embodiment of the third aspect. The public parameter and some other information are required by the predicate encryption algorithm of the fourth embodiment of the third aspect. For specific information required, see Non-patent literature 2, described above, for example.

[0430] In the process of step S17b1, following the process of step S17a, the encryption unit 13 of the encryption apparatus 10 uses the first attribute information $v = (v_1, ..., v_n)$ or the first predicate information $w = (w_1, ..., w_n)$, together with the public key included in the public parameter and the content M read from the memory 11, to obtain encrypted content C_1 according to the predicate encryption algorithm (step S17b1).

[0431] After the process of step S17b1, the process of step 17d is performed. In this process, the transmitter unit 14 of the encryption apparatus 10 generates an encrypted message that includes the encrypted content C_1, and the schema pair, the policy, the public parameter, and the address of the key generation apparatus read from the memory 31, under the control of the controller unit (step S 17d).

[0432] The processes of steps S18 to S26b, following the process of step S17d, are the same as those in the first embodiment of the third aspect.

[0433] When the decryption key is not possessed in the process of step S26b, the second predicate logic information acquisition unit 35 of the decryption apparatus 30 reads the policy, the schema pair, the public parameter, and the user information from the memory 31 and obtains attribute information (called second attribute information) or predicate information (called second predicate information) from the user information (step S27g). In this process, the schema paired with the schema identified by the policy is applied to the user information. When the policy is Cipher_Text_Policy, the schema (attribute schema) paired with the schema (predicate schema) identified by Cipher_Text_Policy is used to obtain the second attribute information from the user information (attribute designation information). When the policy is Key_Policy, the schema (predicate schema) paired with the schema (attribute schema) identified by Key_Policy is used to obtain the second predicate information from the user information (predicate designation information). It should be noted that the schema paired with the schema used in step S17a is used in this process. In the fourth embodiment of the third aspect, the second attribute information and the second predicate information are one or a plurality of vector information having elements of the finite field F_q as components (see Figs. 11 to 13).

[0434] After the process of step S27g, the process of step 27 is performed. In this process, the transmitter unit 34 of the decryption apparatus 30 generates a key request message that includes the public parameter, the policy, the schema

pair, and the authentication information read from the memory 31, and the second attribute information or the second predicate information, under the control of the controller unit. The transmitter unit 34 of the decryption apparatus 30 sends the key request message to the key generation apparatus having the address read from the memory 31, and the receiver unit of the key generation apparatus 20 receives the key request message.

[0435] When the verification succeeds in the process of step S28a, the process of step S28d is performed. Since the key generation apparatus 20 has received the second attribute information or the second predicate information from the decryption apparatus 30, the function and the process for generating the information are unnecessary.

[0436] The process of step S32, following the process of step S28d, is the same as that in the first embodiment of the third aspect.

[0437] In the process of step S26c1, following the process of step S32, the decryption unit 33 of the decryption apparatus 30 reads the public parameter, the decryption key R, and the encrypted content C_1 from the memory 31 to calculate content M according to the predicate encryption algorithm (step S26c1).

[0438] The processes of steps S34 and S35, to be performed after the process of step S26c1, are the same as those in the first embodiment of the third aspect.

[0439] The relay unit decrypts the encrypted content as clearly understood from the above described embodiments of the third aspect. Therefore, decryption can be performed separately from the usual protocol of, for example, a WWW server or a WWW browser, and a known WWW system can be used easily. Since the relay unit performs decryption even when the user does not perform any operation to decrypt the encrypted content, the user is provided with great convenience.

[0440] In the above described embodiments of the third aspect, a cache server may be provided at the communication path between the content server 60 and the decryption apparatus 30 (in that case, the encrypted content is cached).

[0441] The relay unit may cache the encrypted content before it is decrypted, in order to provide convenience when a client terminal is not always connected to the communication network 5.

[0442] To avoid the caching operation of a WWW browser for the decrypted content, an HTTP cache control header that disables caching may be added to a response to the WWW browser.

[0443] When a plurality of users use the same client terminal, the relay unit may have an authentication function. In that case, basic authentication and digest authentication in HTTP may be used for a WWW browser, and an authentication information (user IDs and passwords) table and a management function for adding, changing, and deleting authentication information may be added to the relay unit.

[0444] It is preferred that the above described embodiments of the third aspect be applied to content delivery systems. Since predicate encryption is not based on information depending on the receiver, it is preferred that the predicate encryption be applied to access control of content that may be browsed by unspecified persons.

[0445] Fig. 82 shows the structure of data exchanged. The basic format of the entire message conforms, for example, to S/MIME (Secure Multipurpose Internet Mail Extensions). An appropriate data structure is given to data from the start position marker of an encrypted message to the end position marker of the encrypted message in XML (the extensible Markup Language) or other some language.

[0446] Data related to the encrypted content is called an encryption block. The components of the encryption block will be described below.

[0447] An algorithm identifier block specifies information that identifies the predicate encryption algorithm used to encrypt the private key and the private key encryption algorithm used to encrypt the content. An identifier indicating the algorithm or the version of an algorithm (for example, PE/Version X + Camellia (Camellia is a registered trademark)) can be specified.

[0448] A digital signature block specifies the digital signature. A known signature algorithm can be used. This item can be omitted depending on the application.

[0449] A public parameter information block specifies information that identifies the public parameter used. An identifier that identifies the public parameter or the data of the public parameter can be specified.

[0450] A policy field specifies an identifier that identifies the policy used.

[0451] A schema field specifies an identifier that identifies the schema used or the data of the schema.

[0452] An encryption information field specifies the data (encryption information) obtained by encrypting, with the predicate encryption, the private key used to encrypt the content.

[0453] A content file name, a content type, and a content file size specify the file name of the content, the data type (such as text or html) of the content, and the file size of the content, respectively.

[0454] An attribute field and a predicate field specify letter string representations that indicate the attribute and the predicate used for encryption, corresponding to the policy field, respectively. These items can be omitted according to the application.

[0455] The encrypted content generated by encrypting the content is described in encryption data.

[0456] The basic data structure of the content is described with HTML (Hyper Text Markup Language), and the encryption block is specified by a comment statement in HTML.

[0457] The encryption block is given an appropriate data structure with XML (the extensible Markup Language) or other languages.

[0458] When the encrypted content is directly browsed with a browser, comment statements are not displayed, and the other HTML statements are displayed. Therefore, a message indicating that the data includes encrypted content or an error message for a decryption failure may be described in the other HTML statements.

[0459] In the above description, the algebraic structure S is a finite field. The algebraic structure may be a finite ring (integer residue ring). When a predicate encryption algorithm uses an inner product, for example, the first and second attribute information and the first and second predicate information are vectors having elements of S as components.

[0460] According to the scheme of the algebraic structure S, the public key B is a set of elements of a module V on S, the private key B* is a set of elements of a module V* dual of the module V, and the decryption key R is an element of the dual module V*. When the algebraic structure S is a finite field, the module V on the finite field is a so-called vector space on the finite field. In that case, the encryption unit performs calculations that include a scalar multiplication in which the elements of the public key B are multiplied by the components, used as coefficients, of the first attribute information or a scalar multiplication in which the elements of the public key B are multiplied by the components, used as coefficients, of the first predicate information, to obtain encryption information. The key generation unit performs calculations that include a scalar multiplication in which the elements of the private key B* are multiplied by the components, used as coefficients, of the second predicate information or a scalar multiplication in which the elements of the private key B* are multiplied by the components, used as coefficients, of the second attribute information, to obtain the decryption key R.

[0461] The hardware entities (the client apparatus, the key generation apparatus, the registration apparatus, the management apparatus, the maintenance apparatus, the authentication apparatus, and the content server) included in the cryptographic system include an input unit connectable to a keyboard or the like, an output unit connectable to a liquid crystal display unit and or like, a communication unit connectable to a communication apparatus (such as a communication cable) with which communications are allowed outside the entities, a CPU (central processing unit) (which may be provided with a cache memory and a register), memories such as a RAM and a ROM, an external storage device (hard disk), and a bus that is connected such that data can be exchanged among the input unit, the output unit, the communication unit, the CPU, the RAM, the ROM, and the external storage unit. If necessary, the hardware entities may be provided with an apparatus (drive) that can read and write data to and from a storage medium such as a CD-ROM. Physical entities provided with such hardware resources include a general purpose computer.

[0462] The external storage device of each hardware entity stores a program required to implement the foregoing functions and data required in the processing of the program (instead of the external storage device, a read only storage device, that is, a ROM, may store the program, for example). Data obtained by the processing of the program and the like are stored in a RAM or the external storage device, if necessary. In the above descriptions, storage devices, such as RAMs and registers, that store calculation results and the addresses of the storage areas of the results are called just memories.

[0463] In each hardware entity, the program stored in the external storage device (or the ROM) and the data required for the processing of the program are read into a memory, when needed, and are interpreted, executed, or processed by the CPU, as required. As a result, the CPU implements the predetermined functions (such as those of the encryption unit, the decryption unit, the key generation unit, the first predicate logic information acquisition unit, the second predicate logic information acquisition unit, and the control unit) .

[0464] Numerical calculations in number theory are required in some cases in detailed operations of the hardware entities described in each embodiment. Since the numerical calculations in number theory are performed in the same way as with a known technology, a detailed description thereof, including a calculation method thereof, is omitted. (Software that is capable of the numerical calculations in number theory and indicates the current technical level thereof includes PARI/GP and KANT/KASH. For PARI/GP, see http://pari.math.u-bordeaux.fr/, retrieved on April 14, 2009. For KANT/KASH, see http://www.math.tu-berlin.de/algebra/, retrieved on April 14, 2009.) The following reference A describes the numerical calculations in number theory.

Reference A: H. Cohen, "A Course in Computational Algebraic Number Theory", GTM 138, Springer-Verlag, 1993.

[0465] The present invention is not limited to the embodiments described above, and appropriate modifications can be made without departing from the scope of the present invention. The processes described in the above embodiments may be executed not only time sequentially according to the order of description but also in parallel or individually when necessary or according to the processing capabilities of the apparatuses that execute the processes.

[0466] When the processing functions of the hardware entities described in the above embodiments are implemented by a computer, the processing details of the functions that should be provided by hardware entities are described in a program. When the program is executed by a computer, the processing functions of the hardware entities are implemented on the computer.

[0467] The program containing the processing details can be recorded in a computer-readable storage medium. The computer-readable storage medium can be any type of medium, such as a magnetic storage device, an optical disc, a

magneto-optical storage medium, and a semiconductor memory. For example, a hard disk device, a flexible disk, a magnetic tape, or the like can be used as a magnetic recording device; a digital versatile disc (DVD), a DVD random access memory (DVD-RAM), a compact disc read only memory (CD-ROM), a CD recordable or rewritable (CD-R/RW), or the like can be used as an optical disc; a magneto-optical disc or the like can be used as a magneto-optical storage medium; and an electronically erasable and programmable read only memory (EEPROM) or the like can be used as a semiconductor memory.

[0468] The program is distributed by selling, transferring, or lending a portable recording medium such as a DVD or a CD-ROM with the program recorded on it, for example. The program may also be distributed by storing the program in a storage unit of a server computer and transferring the program from the server computer to another computer through the network.

[0469] A computer that executes this type of program first stores the program recorded on the portable recording medium or the program transferred from the server computer in its storage unit. Then, the computer reads the program stored in its storage unit and executes processing in accordance with the read program. In a different program execution form, the computer may read the program directly from the portable recording medium and execute processing in accordance with the program, or the computer may execute processing in accordance with the program each time the computer receives the program transferred from the server computer. Alternatively, the processing may be executed by a so-called application service provider (ASP) service, in which the processing function is implemented just by giving a program execution instruction and obtaining the results without transferring the program from the server computer to the computer. The program of this form includes information that is provided for use in processing by a computer and is treated correspondingly as a program (something that is not a direct instruction to the computer but is data or the like that has characteristics that determine the processing executed by the computer).

[0470] In the description given above, the hardware entities are implemented by executing the predetermined program on the computer, but at least a part of the processing may be implemented by hardware.

[0471] Information described in figures, such as names, are imaginary and has no relationship with actual persons.

<Summing up>

[0472] The present invention can be summed up from the first aspect in the following way.

Item 1

[0473] A cryptographic system that uses predicate encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;

each of the one or the plurality of key generation apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and
each of the one or the plurality of decryption apparatuses comprises a decryption unit adapted to use the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm.

Item 2

[0474] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;
each of the one or the plurality of decryption apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a decryption unit adapted to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm; and
each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

Item 3

[0475] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;

wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm;
each of the one or the plurality of key generation apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and
each of the one or the plurality of decryption apparatuses comprises a decryption unit adapted to use the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm.

Item 4

[0476] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public

key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm;
each of the one or the plurality of decryption apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a decryption unit adapted to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm; and
each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

Item 5

[0477] A cryptographic system according to one of Items 1 and 2,
wherein the encryption unit of the encryption apparatus encrypts plaintext with the common key to obtain ciphertext; and
the decryption unit of the decryption apparatus uses the common key obtained in the decryption process to apply a second decryption process to the ciphertext or uses a common key generated from the information that is obtained in the decryption process and that is used to generate the common key to apply a second decryption process to the ciphertext.

Item 6

[0478] A cryptographic system according to one of Items 1 to 5,
wherein the attribute designation information and/or the logical expression designation information corresponding to the user is stored in a storage medium; and
the decryption apparatus comprises a user information acquisition unit adapted to acquire the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from the storage medium.

Item 7

[0479] A cryptographic system according to one of Items 1 and 3, wherein the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus, the information being used by the key generation apparatus, is obtained from the decryption apparatus.

Item 8

[0480] A cryptographic system according to one of Items 1 to 6,
wherein the cryptographic system further comprises one or a plurality of user information management apparatuses;
each of the one or the plurality of user information management apparatuses comprises a storage unit adapted to store the attribute designation information and/or the logical expression designation information corresponding to the user; and
the key generation apparatus obtains the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from the user information management apparatus.

Item 9

[0481] A cryptographic system according to one of Items 1 to 8,
wherein the one or the plurality of conversion rule information pairs are determined in advance for each of the one or the plurality of key generation apparatuses;
the cryptographic system further comprises one or a plurality of conversion rule information pair management apparatuses;
each of the one or the plurality of conversion rule information pair management apparatuses comprises a storage unit adapted to store the conversion rule information pair corresponding to each of the one or the plurality of key generation apparatuses;
the encryption apparatus comprises a conversion rule information pair acquisition unit adapted to acquire the conversion rule information pair from the conversion rule information pair management apparatus; and
the decryption apparatus comprises a conversion rule information pair acquisition unit adapted to acquire the conversion

rule information pair from the conversion rule information pair management apparatus

Item 10

[0482] A cryptographic system according to one of Items 1 to 8,
wherein the one or the plurality of conversion rule information pairs are determined in advance for each of the one or the plurality of key generation apparatuses;
each of the one or the plurality of key generation apparatuses further comprises a storage unit adapted to store the conversion rule information pair corresponding to the key generation apparatus;
each of the one or the plurality of encryption apparatuses further comprises a storage unit adapted to store the conversion rule information pair corresponding to at least one of the one or the plurality of the key generation apparatuses; and
each of the one or the plurality of decryption apparatuses further comprises a storage unit adapted to store the conversion rule information pair corresponding to at least one of the one or the plurality of the key generation apparatuses.

Item 11

[0483] A cryptographic system according to one of Items 1 to 10, wherein whether the policy information identifies only the attribute conversion rule information, only the logical expression conversion rule information, or the attribute conversion rule information and the logical expression conversion rule information is determined in advance for each of the one or the plurality of key generation apparatuses.

Item 12

[0484] A cryptographic system according to one of Items 1 to 11,
wherein an algebraic structure K is a finite ring or a finite field;
the first and second attribute information and the first and second logic information are vectors having elements of K as components; and
the decryption process of the decryption unit receives the encryption information and the decryption key as inputs and performs a calculation depending on the result of the canonical inner product of the first logic information and the second attribute information, or of the canonical inner product of the first attribute information and the second logic information.

Item 13

[0485] A cryptographic system according to Item 12,
wherein the public key is a set of elements of a module V on K;
the private key is a set of elements of a module V* dual of the module V;
the decryption key is an element of the dual module V*;
the encryption unit performs calculations that include a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first attribute information or a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first logic information, to obtain the encryption information;
the key generation unit performs calculations that include a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second logic information or a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second attribute information, to obtain the decryption key; and
the calculation used in the decryption process of the decryption unit has bilinearity and the result of the calculation depends on the result of the canonical inner product of the first logic information and the second attribute information, or of the first attribute information and the second logic information, all the pieces of information being taken out from the encryption information and the decryption key according to bilinearity.

Item 14

[0486] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one

or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of each of the one or the plurality of key generation apparatuses;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of each of the one or the plurality of decryption apparatuses.

Item 15

[0487] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to

obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;

a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;

a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and

a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the decryption apparatus.

Item 16

[0488] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least

one or a plurality of encryption apparatuses;

one or a plurality of key generation apparatuses; and

one or a plurality of decryption apparatuses;

wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;

one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and

policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;

the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;

a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of each of the one or the plurality of key generation apparatuses;

a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and

a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of each of the one or the plurality of decryption apparatuses.

Item 17

[0489] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the decryption apparatus.

Item 18

[0490] A cryptographic communication method according to one of Items 14 and 15,
wherein the encryption step comprises a ciphertext generation step of also encrypting plaintext with the common key to obtain ciphertext, in the encryption unit; and
the decryption step comprises a second decryption step of performing a second decryption process of the ciphertext with the common key obtained in the decryption process or a second decryption process of the ciphertext with a common key generated from the information used to generate the common key and obtained in the decryption process, in the decryption unit.

Item 19

[0491] A cryptographic communication method according to one of Items 14 to 18, comprising an acquisition step of acquiring the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from a storage medium that stores the attribute designation information and/or the logical expression designation information corresponding to the user, in an acquisition unit of the decryption apparatus.

Item 20

[0492] A cryptographic communication method according to one of Items 14 and 16, comprising a user information transmission step of transmitting the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus, to the key generation apparatus, in a transmitter unit of the decryption apparatus; and
a user information receiving step of receiving the attribute designation information or the logical expression designation information corresponding to the user from the decryption apparatus, in a receiver unit of the key generation apparatus.

Item 21

[0493] A cryptographic communication method according to one of Items 14 to 18,
wherein the cryptographic system comprises one or a plurality of user information management apparatuses provided with a storage unit adapted to store the attribute designation information and/or the logical expression designation information corresponding to the user; and
the cryptographic communication method comprises a user information acquisition step of acquiring the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from the user information management apparatus, in a user information acquisition unit of the key generation apparatus.

Item 22

[0494] A cryptographic communication method according to one of Items 14 to 21,
wherein the one or the plurality of conversion rule information pairs are determined in advance for each of the one or the plurality of key generation apparatuses;
the cryptographic system comprises one or a plurality of conversion rule information pair management apparatuses provided with a storage unit adapted to store the conversion rule information pair corresponding to each of the one or the plurality of key generation apparatuses; and
the cryptographic communication method comprises:

a conversion rule information pair acquisition step of acquiring the conversion rule information pair from the conversion rule information pair management apparatus, in a conversion rule information pair acquisition unit of the encryption apparatus; and
a conversion rule information pair acquisition step of acquiring the conversion rule information pair from the conversion rule information pair management apparatus, in a conversion rule information pair acquisition unit of the decryption apparatus.

Item 23

[0495] A cryptographic communication method according to one of Items 14 to 22, wherein whether the policy information identifies only the attribute conversion rule information, only the logical expression conversion rule information, or the attribute conversion rule information and the logical expression conversion rule information is determined in advance for each of the one or the plurality of key generation apparatuses.

Item 24

[0496] A cryptographic communication method according to one of Items 14 to 23,
wherein an algebraic structure K is a finite ring or a finite field;
the first and second attribute information and the first and second logic information are vectors having elements of K as components; and
in the decryption step, the encryption information and the decryption key serve as inputs and a calculation is performed depending on the result of the canonical inner product of the first logic information and the second attribute information, or of the canonical inner product of the first attribute information and the second logic information, in the decryption unit.

Item 25

[0497] A cryptographic communication method according to Item 24,
wherein the public key is a set of elements of a module V on K;

the private key is a set of elements of a module V* dual of the module V;
the decryption key is an element of the dual module V*;
in the encryption step, calculations that include a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first attribute information or a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first logic information, are performed to obtain the encryption information, in the encryption unit;
in the key generation step, calculations that include a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second logic information or a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second attribute information, are performed to obtain the decryption key, in the key generation unit; and
the calculation used in the decryption process of the decryption unit has bilinearity and the result of the calculation depends on the result of the canonical inner product of the first logic information and the second attribute information, or of the first attribute information and the second logic information, all the pieces of information being taken out from the encryption information and the decryption key according to bilinearity.

Item 26

[0498] An encryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the encryption apparatus comprising:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm.

Item 27

[0499] An encryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression des-

ignation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the encryption apparatus comprising:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm.

Item 28

[0500] A key generation apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the key generation apparatus comprising:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

Item 29

[0501] A key generation apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;

the key generation apparatus comprising a key generation unit adapted to use the private key of the key generation apparatus, together with attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) generated from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus by using the conversion rule information paired with the conversion rule information identified by the policy information, to generate a decryption key used to decrypt the encryption information.

Item 30

[0502] A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising a decryption unit adapted to use a decryption key generated by the key generation apparatus to apply a decryption process to encryption information generated by the encryption apparatus, according to the functional encryption algorithm.

Item 31

[0503] A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a decryption unit adapted to use a decryption key generated by the key generation apparatus to apply a decryption process to encryption information generated by the encryption apparatus, according to the functional encryption algorithm.

Item 32

[0504] A program for making a computer function as an encryption apparatus according to one of Items 26 and 27.

Item 33

[0505] A program for making a computer function as a key generation apparatus according to one of Items 28 and 29.

Item 34

[0506] A program for making a computer function as a decryption apparatus according to one of Items 30 and 31.

Item 35

[0507] A computer readable storage medium having stored thereon at least one of a program according to Item 32, a program according to Item 33, and a program according to Item 34.

[0508] The present invention can be summed up from the second aspect in the following way. In the following description, item numbers will start again at one.

Item 1

[0509] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of each of the one or the plurality of key generation apparatuses;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption

information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

Item 2

[0510] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus,

in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of the first decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the first decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the first decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the second decryption apparatus;
a logic information transmission step of transmitting the third attribute information or the third logic information to the key generation apparatus, in a transmitter unit of the second decryption apparatus;
a logic information receiving step of receiving the third attribute information or the third logic information from the second decryption apparatus, in the receiver unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

Item 3

[0511] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression des-

ignation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of each of the one or the plurality of key generation apparatuses;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

Item 4

[0512] A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of the first decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the first decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the first decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the second decryption apparatus;
a logic information transmission step of transmitting the third attribute information or the third logic information to

the key generation apparatus, in a transmitter unit of the second decryption apparatus;
a logic information receiving step of receiving the third attribute information or the third logic information from the second decryption apparatus, in the receiver unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

Item 5

[0513] A cryptographic communication method according to one of Items 1 and 2,
wherein the encryption step comprises a ciphertext generation step of also encrypting plaintext with the common key to obtain ciphertext, in the encryption unit; and
the decryption step comprises a second decryption step of performing a second decryption process of the ciphertext with the common key obtained in the decryption process or a second decryption process of the ciphertext with a common key generated from the information used to generate the common key and obtained in the decryption process, in the decryption unit.

Item 6

[0514] A cryptographic communication method according to one of Items 1 to 5, comprising an acquisition step of acquiring the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from a storage medium that stores the attribute designation information and/or the logical expression designation information corresponding to the user, in an acquisition unit of the decryption apparatus.

Item 7

[0515] A cryptographic communication method according to one of Items 1 and 3, comprising a user information transmission step of transmitting the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus, to the key generation apparatus, in a transmitter unit of the decryption apparatus; and
a user information receiving step of receiving the attribute designation information or the logical expression designation information corresponding to the user from the decryption apparatus, in a receiver unit of the key generation apparatus.

Item 8

[0516] A cryptographic communication method according to one of Items 1 to 6,
wherein the cryptographic system comprises one or a plurality of user information management apparatuses provided with a storage unit adapted to store the attribute designation information and/or the logical expression designation information corresponding to the user; and
the cryptographic communication method comprises a user information acquisition step of acquiring the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from the user information management apparatus, in a user information acquisition unit of the key generation apparatus.

Item 9

[0517] A cryptographic communication method according to one of Items 1 to 8,
wherein the one or the plurality of conversion rule information pairs are determined in advance for each of the one or the plurality of key generation apparatuses;
the cryptographic system comprises one or a plurality of conversion rule information pair management apparatuses provided with a storage unit adapted to store the conversion rule information pair corresponding to each of the one or the plurality of key generation apparatuses; and

the cryptographic communication method comprises:

a conversion rule information pair acquisition step of acquiring the conversion rule information pair from the conversion rule information pair management apparatus, in a conversion rule information pair acquisition unit of the encryption apparatus; and
a conversion rule information pair acquisition step of acquiring the conversion rule information pair from the conversion rule information pair management apparatus, in a conversion rule information pair acquisition unit of the decryption apparatus.

Item 10

[0518] A cryptographic communication method according to one of Items 1 to 9, wherein whether the policy information identifies only the attribute conversion rule information, only the logical expression conversion rule information, or the attribute conversion rule information and the logical expression conversion rule information is determined in advance for each of the one or the plurality of key generation apparatuses.

Item 11

[0519] A cryptographic communication method according to one of Items 1 to 10,
wherein an algebraic structure K is a finite ring or a finite field;
the first and second attribute information and the first and second logic information are vectors having elements of K as components; and
in the decryption step, the encryption information and the decryption key serve as inputs and a calculation is performed depending on the result of the canonical inner product of the first logic information and the second attribute information, or of the canonical inner product of the first attribute information and the second logic information, in the decryption unit.

Item 12

[0520] A cryptographic communication method according to Item 11,
wherein the public key is a set of elements of a module V on K;
the private key is a set of elements of a module V* dual of the module V;
the decryption key is an element of the dual module V*;
in the encryption step, calculations that include a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first attribute information or a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first logic information, are performed to obtain the encryption information, in the encryption unit;
in the key generation step, calculations that include a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second logic information or a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second attribute information, are performed to obtain the decryption key, in the key generation unit; and
the calculation used in the decryption process of the decryption unit has bilinearity and the result of the calculation depends on the result of the canonical inner product of the first logic information and the second attribute information, or of the first attribute information and the second logic information, all the pieces of information being taken out from the encryption information and the decryption key according to bilinearity.

Item 13

[0521] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a

conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;
each of the one or the plurality of key generation apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and
the decryption apparatus comprises
a decryption unit adapted to use the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm; and
a transfer unit adapted to transfer the encryption information to at least one decryption apparatus other than the decryption apparatus.

Item 14

[0522] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption

algorithm;
the decryption apparatus comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;
a decryption unit adapted to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm; and
a transfer unit adapted to transfer the encryption information to at least one decryption apparatus other than the decryption apparatus; and
each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

Item 15

[0523] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm;
each of the one or the plurality of key generation apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and
the decryption apparatus comprises
a decryption unit adapted to use the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm; and
a transfer unit adapted to transfer the encryption information to at least one decryption apparatus other than the decryption apparatus.

Item 16

[0524] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm;
the decryption apparatus comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;
a decryption unit adapted to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm; and
a transfer unit adapted to transfer the encryption information to at least one decryption apparatus other than the decryption apparatus; and
each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

Item 17

[0525] A cryptographic system according to one of Items 13 and 14,
wherein the encryption unit of the encryption apparatus encrypts plaintext with the common key to obtain ciphertext; and the decryption unit of the decryption apparatus uses the common key obtained in the decryption process to apply a second decryption process to the ciphertext or uses a common key generated from the information that is obtained in the decryption process and that is used to generate the common key to apply a second decryption process to the ciphertext.

Item 18

[0526] A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information

(hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:

a decryption unit adapted to use a decryption key generated by the key generation apparatus to apply a decryption process to encryption information generated by the encryption apparatus, according to the functional encryption algorithm; and
a transfer unit adapted to transfer the encryption information to at least one decryption apparatus other than the decryption apparatus.

Item 19

[0527] A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;
a decryption unit adapted to use a decryption key generated by the key generation apparatus to apply a decryption process to encryption information generated by the encryption apparatus, according to the functional encryption algorithm; and
a transfer unit adapted to transfer the encryption information to at least one decryption apparatus other than the decryption apparatus.

Item 20

[0528] A program for making a computer function as a decryption apparatus according to one of Items 18 and 19.

Item 21

[0529] A computer readable storage medium having stored thereon a program according to Item 20.

[0530] The present invention can be summed up from the third aspect in the following way. In the following description, item numbers will start again at one.

Item 1

[0531] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;

one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm;
each of the one or the plurality of content servers comprises
a storage unit adapted to store the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus;
each of the one or the plurality of key generation apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and
each of the one or the plurality of decryption apparatuses comprises
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, to use the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and to use the common key obtained in the decryption process to perform a content acquisition process for decrypting the encrypted content obtained from the content server.

Item 2

[0532] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that

designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;

policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;

each of the one or the plurality of encryption apparatuses comprises

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and

an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm;

each of the one or the plurality of content servers comprises

a storage unit adapted to store the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and

a transmitter unit adapted to transmit the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus;

each of the one or the plurality of decryption apparatuses comprises

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;

a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and

a relay unit adapted to send to the content server the acquisition request sent from the browser unit, to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and to use the common key obtained in the decryption process to perform a content acquisition process for decrypting the encrypted content obtained from the content server; and

each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

Item 3

[0533] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;

one or a plurality of key generation apparatuses;

one or a plurality of decryption apparatuses; and

one or a plurality of content servers;

wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;

one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;

policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;

each of the one or the plurality of encryption apparatuses comprises

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm;
each of the one or the plurality of content servers comprises
a storage unit adapted to store the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus;
each of the one or the plurality of key generation apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encrypted content; and
each of the one or the plurality of decryption apparatuses comprises
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, and to use the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm.

Item 4

[0534] A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises
a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to

the functional encryption algorithm;
each of the one or the plurality of content servers comprises
a storage unit adapted to store the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus;
each of the one or the plurality of decryption apparatuses comprises
a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, and to use a decryption key sent from the key generation apparatus to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm; and
each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encrypted content.

Item 5

[0535] A cryptographic system according to one of Items 1 to 4,
wherein the attribute designation information and/or the logical expression designation information corresponding to the user is stored in a storage medium; and
the decryption apparatus comprises a user information acquisition unit adapted to acquire the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from the storage medium.

Item 6

[0536] A cryptographic system according to one of Items 1 and 3, wherein the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus, the information being used by the key generation apparatus, is obtained from the decryption apparatus.

Item 7

[0537] A cryptographic system according to one of Items 1 to 6,
wherein the cryptographic system further comprises one or a plurality of user information management apparatuses;
each of the one or the plurality of user information management apparatuses comprises a storage unit adapted to store the attribute designation information and/or the logical expression designation information corresponding to the user; and
the key generation apparatus obtains the attribute designation information or the logical expression designation information corresponding to the user of the decryption apparatus from the user information management apparatus.

Item 8

[0538] A cryptographic system according to one of Items 1 to 7,
wherein the one or the plurality of conversion rule information pairs are determined in advance for each of the one or the plurality of key generation apparatuses;
the cryptographic system further comprises one or a plurality of conversion rule information pair management apparatuses;
each of the one or the plurality of conversion rule information pair management apparatuses comprises a storage unit adapted to store the conversion rule information pair corresponding to each of the one or the plurality of key generation apparatuses;
the encryption apparatus comprises a conversion rule information pair acquisition unit adapted to acquire the conversion rule information pair from the conversion rule information pair management apparatus; and
the decryption apparatus comprises a conversion rule information pair acquisition unit adapted to acquire the conversion rule information pair from the conversion rule information pair management apparatus

Item 9

[0539] A cryptographic system according to one of Items 1 to 7,
wherein the one or the plurality of conversion rule information pairs are determined in advance for each of the one or the plurality of key generation apparatuses;
each of the one or the plurality of key generation apparatuses further comprises a storage unit adapted to store the conversion rule information pair corresponding to the key generation apparatus;
each of the one or the plurality of encryption apparatuses further comprises a storage unit adapted to store the conversion rule information pair corresponding to at least one of the one or the plurality of the key generation apparatuses; and
each of the one or the plurality of decryption apparatuses further comprises a storage unit adapted to store the conversion rule information pair corresponding to at least one of the one or the plurality of the key generation apparatuses.

Item 10

[0540] A cryptographic system according to one of Items 1 to 9, wherein whether the policy information identifies only the attribute conversion rule information, only the logical expression conversion rule information, or the attribute conversion rule information and the logical expression conversion rule information is determined in advance for each of the one or the plurality of key generation apparatuses.

Item 11

[0541] A cryptographic system according to one of Items 1 to 10,
wherein an algebraic structure K is a finite ring or a finite field;
the first and second attribute information and the first and second logic information are vectors having elements of K as components; and
the decryption process of the decryption unit performs a calculation depending on the result of the canonical inner product of the first logic information and the second attribute information, or of the canonical inner product of the first attribute information and the second logic information.

Item 12

[0542] A cryptographic system according to Item 11,
wherein the public key is a set of elements of a module V on K;
the private key is a set of elements of a module V* dual of the module V;
the decryption key is an element of the dual module V*;
the encryption unit performs calculations that include a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first attribute information or a scalar multiplication in which the elements of the public key are multiplied by the components, used as coefficients, of the first logic information, to obtain the encryption information;
the key generation unit performs calculations that include a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second logic information or a scalar multiplication in which the elements of the private key are multiplied by the components, used as coefficients, of the second attribute information, to obtain the decryption key; and
the calculation used in the decryption process of the decryption unit has bilinearity and the result of the calculation depends on the result of the canonical inner product of the first logic information and the second attribute information, or of the first attribute information and the second logic information, all the pieces of information being taken out from the encryption information or the encrypted content, and the decryption key according to bilinearity.

Item 13

[0543] A cryptographic communication method for a cryptographic system that uses functional encryption and includes: at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;

one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto to the content server, in a transmitter unit of the encryption apparatus;
a storing step of storing the encryption information and the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content and the encryption information from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of each of the one or the plurality of key generation apparatuses;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;
a decryption step of using the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and of using the common key obtained in the decryption process to perform a content acquisition process in which the encrypted content obtained from the content server is decrypted, in a relay unit of the decryption apparatus; and
a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

Item 14

[0544] A cryptographic communication method for a cryptographic system that uses functional encryption and includes:

at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto to the content server, in a transmitter unit of the encryption apparatus;
a storing step of storing the encryption information and the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content and the encryption information from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit

of the decryption apparatus;
a decryption step of using the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and of using the common key obtained in the decryption process to perform a content acquisition process in which the encrypted content obtained from the content server is decrypted, in a relay unit of the decryption apparatus; and
a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

Item 15

[0545] A cryptographic communication method for a cryptographic system that uses functional encryption and includes: at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
a transmission step of transmitting the encrypted content to the content server, in a transmitter unit of the encryption apparatus;
a storing step of storing the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of each of the one or the plurality of key generation apparatuses;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encrypted content,

in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;
a decryption step of using the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm, in a relay unit of the decryption apparatus; and
a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

Item 16

[0546] A cryptographic communication method for a cryptographic system that uses functional encryption and includes: at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:
a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of each of the one or the plurality of encryption apparatuses;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto to the content server, in a transmitter unit of the encryption apparatus;
a storing step of storing the encryption information and the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content and the encryption information from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to

the key generation apparatus, in a transmitter unit of the decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;
a decryption step of using the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and of using the private key obtained in the decryption process to perform a content acquisition process in which the encrypted content obtained from the content server is decrypted, in a relay unit of the decryption apparatus; and
a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

Item 17

[0547] A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting content with the common key, according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers that store the encrypted content and the encryption information,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in the functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, to use the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and to use the common key obtained in the decryption process to perform a content acquisition process for decrypting the encrypted content obtained from the content server.

Item 18

[0548] A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that encrypt content to obtain encrypted content according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers that store the encrypted content,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in the functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression des-

ignation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit and to use the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm.

Item 19

[0549] A content server used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting content with the common key, according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers;
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the content server comprising:
a storage unit adapted to store the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus.

Item 20

[0550] A content server used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that encrypt content to obtain encrypted content according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers;
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the content server comprising:
a storage unit adapted to store the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus.

Item 21

[0551] A program for making a computer function as a decryption apparatus according to one of Items 17 and 18.

Item 22

[0552] A program for making a computer function as a content server according to one of Items 19 and 20.

Item 23

[0553] A computer readable storage medium having stored thereon a program according to Item 21 and/or a program according to Item 22.

Claims

1. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;

each of the one or the plurality of key generation apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and

each of the one or the plurality of decryption apparatuses comprises a decryption unit adapted to use the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm.

2. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm;

each of the one or the plurality of decryption apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a decryption unit adapted to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm; and

each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

3. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting in-

formation that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm;

each of the one or the plurality of key generation apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and

each of the one or the plurality of decryption apparatuses comprises a decryption unit adapted to use the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm.

4. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information ac-

cording to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and

an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext according to the functional encryption algorithm;

each of the one or the plurality of decryption apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and

a decryption unit adapted to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information according to the functional encryption algorithm; and

each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

5. A cryptographic system according to Claim 1,
wherein the encryption unit of the encryption apparatus encrypts plaintext with the common key to obtain ciphertext; and
the decryption unit of the decryption apparatus uses the common key obtained in the decryption process to apply a second decryption process to the ciphertext or uses a common key generated from the information that is obtained in the decryption process to apply a second decryption process to the ciphertext.

6. A cryptographic system according to Claim 2,
wherein the encryption unit of the encryption apparatus encrypts plaintext with the common key to obtain ciphertext; and
the decryption unit of the decryption apparatus uses the common key obtained in the decryption process to apply a second decryption process to the ciphertext or uses a common key generated from the information that is obtained in the decryption process to apply a second decryption process to the ciphertext.

7. A cryptographic system according to one of Claims 1 to 6,
wherein the cryptographic system comprises the plurality of decryption apparatuses; and
at least one decryption apparatus of the plurality of decryption apparatuses comprises a transfer unit for transferring the encryption information to at least one decryption apparatus of the plurality of decryption apparatuses, other than the decryption apparatus.

8. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression

conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm;

each of the one or the plurality of content servers comprises:

a storage unit adapted to store the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus;

each of the one or the plurality of key generation apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information; and

each of the one or the plurality of decryption apparatuses comprises:

a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, to use the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and to use the common key obtained in the decryption process to perform a content acquisition process for decrypting the encrypted content obtained from the content server.

9. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (here-

after called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm;

each of the one or the plurality of content servers comprises:

a storage unit adapted to store the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus;

each of the one or the plurality of decryption apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, to use a decryption key sent from the key generation apparatus to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and to use the common key obtained in the decryption process to perform a content acquisition process for decrypting the encrypted content obtained from the content server; and

each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encryption information.

10. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule

information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm;

each of the one or the plurality of content servers comprises:

a storage unit adapted to store the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus;

each of the one or the plurality of key generation apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encrypted content; and

each of the one or the plurality of decryption apparatuses comprises:

a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, and to use the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm.

11. A cryptographic system that uses functional encryption, comprising at least:

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (here-

after called logical expression designation information) to logic information used in the functional encryption algorithm;
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
each of the one or the plurality of encryption apparatuses comprises:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm;

each of the one or the plurality of content servers comprises:

a storage unit adapted to store the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus;

each of the one or the plurality of decryption apparatuses comprises:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus;
a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, and to use a decryption key sent from the key generation apparatus to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm; and

each of the one or the plurality of key generation apparatuses comprises a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate the decryption key used to decrypt the encrypted content.

12. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;

a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the key generation apparatus;

a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and

a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the decryption apparatus.

13. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least

one or a plurality of encryption apparatuses;

one or a plurality of key generation apparatuses; and

one or a plurality of decryption apparatuses;

wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;

one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and

policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;

the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;

a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;

a key generation step of using the second attribute information or the second logic information, together with

the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the decryption apparatus.

14. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the decryption apparatus.

15. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
one or a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion

rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm, in an encryption unit of the encryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus; and
a decryption step of using the decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the decryption apparatus.

16. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;

a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

17. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of the first decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the first decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the first decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the second decryption apparatus;
a logic information transmission step of transmitting the third attribute information or the third logic information to the key generation apparatus, in a transmitter unit of the second decryption apparatus;
a logic information receiving step of receiving the third attribute information or the third logic information from the second decryption apparatus, in the receiver unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

18. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that

designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

19. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least

one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses; and
a plurality of decryption apparatuses;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
an encryption information transmission step of transmitting the encryption information to a first decryption apparatus, in a transmitter unit of the encryption apparatus;
an encryption information receiving step of receiving the encryption information from the encryption apparatus, in a receiving unit of the first decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the first decryption apparatus, in a second propositional logic information acquisition unit of the first decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the first decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the first decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a first decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the first decryption key to the first decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the first decryption key from the key generation apparatus, in the receiving unit of the first decryption apparatus;
a decryption step of using the first decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the first decryption apparatus;
a transfer step of transferring the encryption information to a second decryption apparatus, other than the first decryption apparatus, in a transfer unit of the first decryption apparatus;
a receiving step of receiving the encryption information from the first decryption apparatus, in a receiving unit of the second decryption apparatus;
a third propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called third attribute information) or logic information (hereafter called third logic information) from attribute designation information or logical expression designation information corresponding to a user of the second decryption apparatus, in the second propositional logic information acquisition unit of the second decryption apparatus;
a logic information transmission step of transmitting the third attribute information or the third logic information

to the key generation apparatus, in a transmitter unit of the second decryption apparatus;
a logic information receiving step of receiving the third attribute information or the third logic information from the second decryption apparatus, in the receiver unit of the key generation apparatus;
a key generation step of using the third attribute information or the third logic information, together with the private key of the key generation apparatus, to generate a second decryption key used to decrypt the encryption information, in the key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the second decryption key to the second decryption apparatus, in the transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the second decryption key from the key generation apparatus, in the receiving unit of the second decryption apparatus; and
a decryption step of using the second decryption key to apply a decryption process to the encryption information according to the functional encryption algorithm in a decryption unit of the second decryption apparatus.

20. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto to the content server, in a transmitter unit of the encryption apparatus;
a storing step of storing the encryption information and the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content and the encryption information from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with

the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the key generation apparatus;

a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;

a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;

a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;

a decryption step of using the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and of using the common key obtained in the decryption process to perform a content acquisition process in which the encrypted content obtained from the content server is decrypted, in a relay unit of the decryption apparatus; and

a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

21. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least

one or a plurality of encryption apparatuses;

one or a plurality of key generation apparatuses;

one or a plurality of decryption apparatuses; and

one or a plurality of content servers;

wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;

one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and

policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;

the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting the content with the common key, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;

a transmission step of transmitting the encrypted content and the encryption information corresponding thereto to the content server, in a transmitter unit of the encryption apparatus;

a storing step of storing the encryption information and the encrypted content sent from the encryption apparatus, in a storage unit of the content server;

an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;

a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;

a transmission step of transmitting the encrypted content and the encryption information corresponding thereto,

in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;

a receiving step of receiving the encrypted content and the encryption information from the content server, in a receiving unit of the decryption apparatus;

a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;

a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the decryption apparatus;

a logic information receiving step of receiving the second attribute information or the second logic information from the decryption apparatus, in a receiver unit of the key generation apparatus;

a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;

a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;

a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;

a decryption step of using the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and of using the common key obtained in the decryption process to perform a content acquisition process in which the encrypted content obtained from the content server is decrypted, in a relay unit of the decryption apparatus; and

a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

22. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least

one or a plurality of encryption apparatuses;

one or a plurality of key generation apparatuses;

one or a plurality of decryption apparatuses; and

one or a plurality of content servers;

wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;

one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and

policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;

the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;

an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content, according to the functional encryption algorithm in an encryption unit of the encryption apparatus;

a transmission step of transmitting the encrypted content to the content server, in a transmitter unit of the encryption apparatus;

a storing step of storing the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encrypted content, in a key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;
a decryption step of using the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm, in a relay unit of the decryption apparatus; and
a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

23. A cryptographic communication method for a cryptographic system that uses functional encryption and includes at least
one or a plurality of encryption apparatuses;
one or a plurality of key generation apparatuses;
one or a plurality of decryption apparatuses; and
one or a plurality of content servers;
wherein a private key and a public key corresponding to the private key are determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs are determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information is determined in advance;
the cryptographic communication method comprising:

a first propositional logic information acquisition step of using one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information, in a first propositional logic information acquisition unit of the encryption apparatus;
an encryption step of using the first attribute information or the first logic information, together with the public key of the key generation apparatus and content, to encrypt the content to obtain encrypted content according to the functional encryption algorithm in an encryption unit of the encryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto

to the content server, in a transmitter unit of the encryption apparatus;
a storing step of storing the encryption information and the encrypted content sent from the encryption apparatus, in a storage unit of the content server;
an acquisition request processing step of performing a process of an acquisition request of the encrypted content for the content server, in a browser unit of the decryption apparatus;
a transmission step of transmitting the acquisition request sent from the browser unit, to the content server, in a relay unit of the decryption apparatus;
a transmission step of transmitting the encrypted content and the encryption information corresponding thereto, in response to the request sent from the decryption apparatus, to the decryption apparatus, in a transmitter unit of the content server;
a receiving step of receiving the encrypted content and the encryption information from the content server, in a receiving unit of the decryption apparatus;
a second propositional logic information acquisition step of using the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus, in a second propositional logic information acquisition unit of the decryption apparatus;
a logic information transmission step of transmitting the second attribute information or the second logic information to the key generation apparatus, in a transmitter unit of the decryption apparatus;
a logic information receiving step of receiving the second attribute information or the second logic information from the decryption apparatus, in a receiver unit of the key generation apparatus;
a key generation step of using the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information, in a key generation unit of the key generation apparatus;
a decryption key transmission step of transmitting the decryption key to the decryption apparatus, in a transmitter unit of the key generation apparatus;
a decryption key receiving step of receiving the decryption key from the key generation apparatus, in a receiver unit of the decryption apparatus;
a decryption step of using the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and of using the private key obtained in the decryption process to perform a content acquisition process in which the encrypted content obtained from the content server is decrypted, in a relay unit of the decryption apparatus; and
a displaying step of displaying content obtained by decrypting the encrypted content, in a browser unit of the decryption apparatus.

24. An encryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the encryption apparatus comprising:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and

an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus, to obtain a common key, and encryption information corresponding to the common key or corresponding to information used to generate the common key, according to the functional encryption algorithm.

25. An encryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the encryption apparatus comprising:

a first propositional logic information acquisition unit adapted to use one kind of conversion rule information of the attribute conversion rule information and the logical expression conversion rule information included in one conversion rule information pair selected from the one or the plurality of conversion rule information pairs, the one kind of conversion rule information being selected together with the policy information according to whether input information input to the encryption apparatus is either attribute designation information or logical expression designation information, to obtain attribute information (hereafter called first attribute information) or logic information (hereafter called first logic information) from the input information; and
an encryption unit adapted to use the first attribute information or the first logic information, together with the public key of the key generation apparatus and plaintext, to obtain encryption information corresponding to the plaintext, according to the functional encryption algorithm.

26. A key generation apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the key generation apparatus comprising:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus; and
a key generation unit adapted to use the second attribute information or the second logic information, together with the private key of the key generation apparatus, to generate a decryption key used to decrypt the encryption information.

27. A key generation apparatus used in a cryptographic system that uses functional encryption and includes, at least,

one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the key generation apparatus comprising a key generation unit adapted to use the private key of the key generation apparatus, together with attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) generated from attribute designation information or logical expression designation information corresponding to a user of the decryption apparatus by using the conversion rule information paired with the conversion rule information identified by the policy information, to generate a decryption key used to decrypt the encryption information.

28. A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising a decryption unit adapted to use a decryption key generated by the key generation apparatus to apply a decryption process to encryption information generated by the encryption apparatus, according to the functional encryption algorithm.

29. A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses, one or a plurality of key generation apparatuses, and one or a plurality of decryption apparatuses,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:

a second propositional logic information acquisition unit adapted to use the conversion rule information paired with the conversion rule information identified by the policy information to obtain attribute information (hereafter called second attribute information) or logic information (hereafter called second logic information) from attribute designation information or logical expression designation information corresponding to a user of the decryption

apparatus; and
a decryption unit adapted to use a decryption key generated by the key generation apparatus to apply a decryption process to encryption information generated by the encryption apparatus, according to the functional encryption algorithm.

30. A decryption apparatus according to one of Claims 28 and 29, further comprising, when the cryptographic system includes the plurality of decryption apparatuses, a transfer unit for transferring the encryption information to at least one decryption apparatus other than the decryption apparatus.

31. A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting content with the common key, according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers that store the encrypted content and the encryption information,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in the functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:

a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit, to use the decryption key to apply a decryption process to the encryption information obtained from the content server, according to the functional encryption algorithm, and to use the common key obtained in the decryption process to perform a content acquisition process for decrypting the encrypted content obtained from the content server.

32. A decryption apparatus used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that encrypt content to obtain encrypted content according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers that store the encrypted content,
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in the functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the decryption apparatus comprising:

a browser unit adapted to perform a process of an acquisition request of the encrypted content for the content server and to display content obtained by decrypting the encrypted content; and
a relay unit adapted to send to the content server the acquisition request sent from the browser unit and to use the decryption key to apply a decryption process to the encrypted content obtained from the content server, according to the functional encryption algorithm.

33. A content server used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that obtain a common key, encryption information corresponding to the common key or corresponding to information used to generate the common key, and encrypted content obtained by encrypting content with the common key, according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers;
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the content server comprising:

a storage unit adapted to store the encryption information and the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content and the encryption information corresponding thereto, in response to a request sent from the decryption apparatus, to the decryption apparatus.

34. A content server used in a cryptographic system that uses functional encryption and includes, at least, one or a plurality of encryption apparatuses that encrypt content to obtain encrypted content according to a functional encryption algorithm; one or a plurality of key generation apparatuses; one or a plurality of decryption apparatuses; and one or a plurality of content servers;
in the cryptographic system,
a private key and a public key corresponding to the private key being determined in advance for each of the one or the plurality of key generation apparatuses;
one or a plurality of conversion rule information pairs being determined in advance, each pair of which has information (hereafter called attribute conversion rule information) prescribing a conversion rule for converting information that designates an attribute (hereafter called attribute designation information) to attribute information used in a functional encryption algorithm and information (hereafter called logical expression conversion rule information) prescribing a conversion rule for converting information that designates a logical expression (hereafter called logical expression designation information) to logic information used in the functional encryption algorithm; and
policy information that identifies one of the attribute conversion rule information and the logical expression conversion rule information being determined in advance;
the content server comprising:

a storage unit adapted to store the encrypted content sent from each of the one or the plurality of encryption apparatuses; and
a transmitter unit adapted to transmit the encrypted content, in response to a request sent from the decryption apparatus, to the decryption apparatus.

35. A program for making a computer function as an encryption apparatus according to one of Claims 24 and 25.

36. A program for making a computer function as a key generation apparatus according to one of Claims 26 and 27.

37. A program for making a computer function as a decryption apparatus according to one of Claims 28, 29, 31, and 32.

38. A program for making a computer function as a content server according to one of Claims 33 and 34.

39. A computer readable storage medium having stored thereon at least one of a program according to Claim 35, a program according to Claim 36, a program according to Claim 37, and a program according to Claim 38.

FIG.1

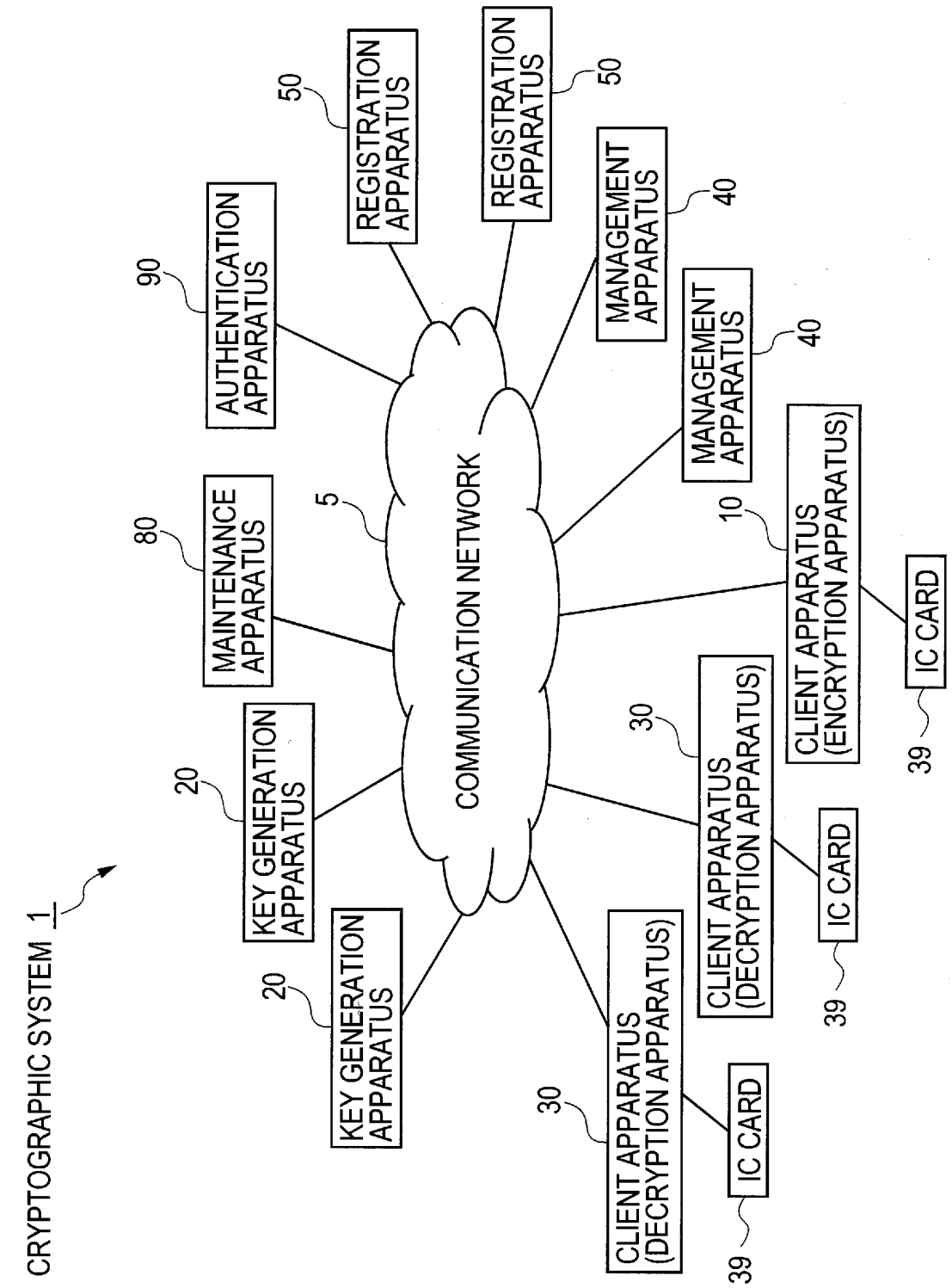

CRYPTOGRAPHIC SYSTEM 1
COMMUNICATION NETWORK
5
AUTHENTICATION APPARATUS
90
REGISTRATION APPARATUS
50
REGISTRATION APPARATUS
50
MANAGEMENT APPARATUS
40
MANAGEMENT APPARATUS
40
MAINTENANCE APPARATUS
80
KEY GENERATION APPARATUS
20
KEY GENERATION APPARATUS
20
CLIENT APPARATUS (ENCRYPTION APPARATUS)
10
IC CARD
39
CLIENT APPARATUS (DECRYPTION APPARATUS)
30
IC CARD
39
CLIENT APPARATUS (DECRYPTION APPARATUS)
30
IC CARD
39

FIG.2

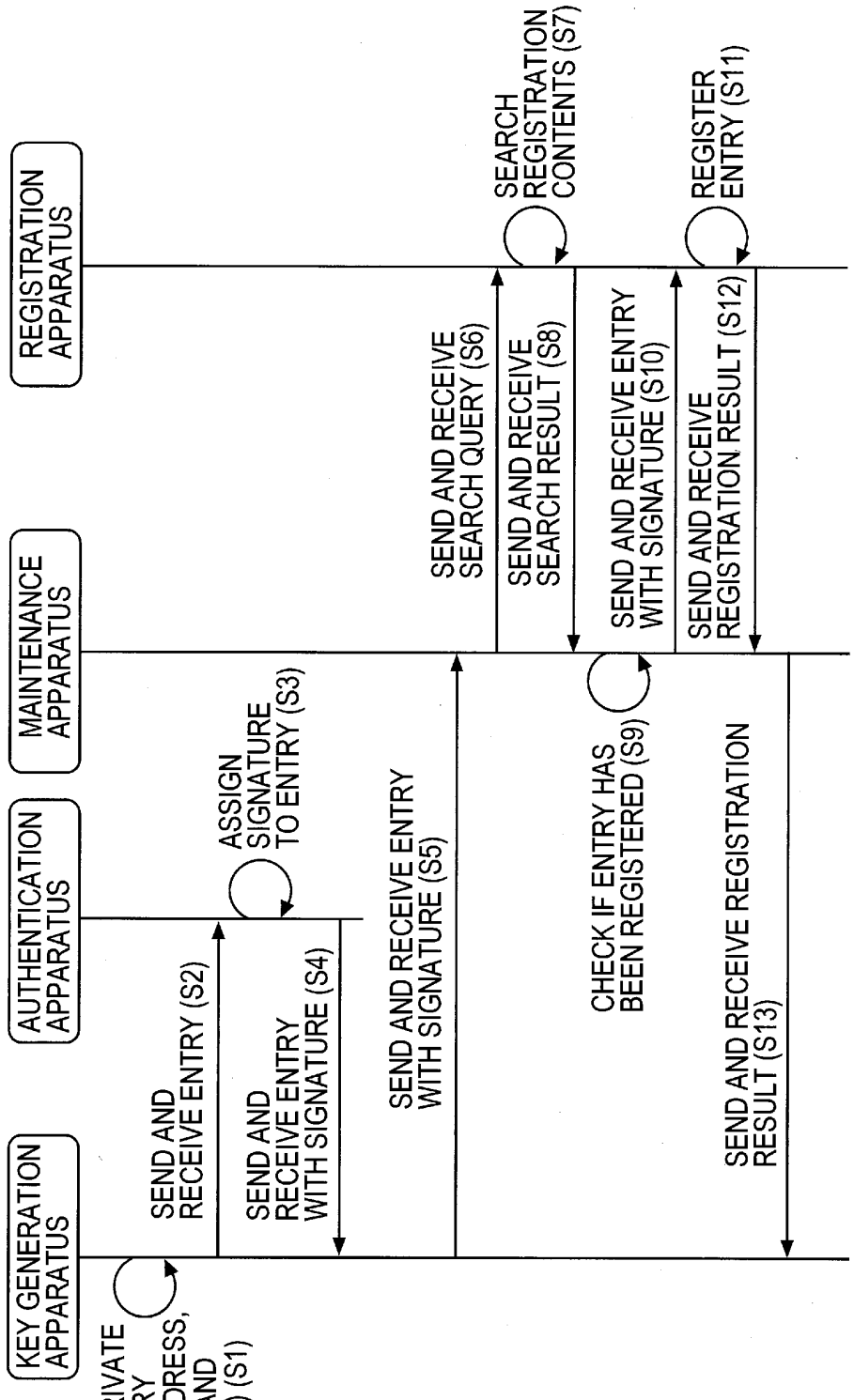

KEY GENERATION APPARATUS
AUTHENTICATION APPARATUS
MAINTENANCE APPARATUS
REGISTRATION APPARATUS
GENERATE PRIVATE KEY AND ENTRY (PUBLIC P, ADDRESS, POLICY LIST AND SCHEMA LIST) (S1)
SEND AND RECEIVE ENTRY (S2)
ASSIGN SIGNATURE TO ENTRY (S3)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S4)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S5)
SEND AND RECEIVE SEARCH QUERY (S6)
SEARCH REGISTRATION CONTENTS (S7)
SEND AND RECEIVE SEARCH RESULT (S8)
CHECK IF ENTRY HAS BEEN REGISTERED (S9)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S10)
REGISTER ENTRY (S11)
SEND AND RECEIVE REGISTRATION RESULT (S12)
SEND AND RECEIVE REGISTRATION RESULT (S13)

FIG.3

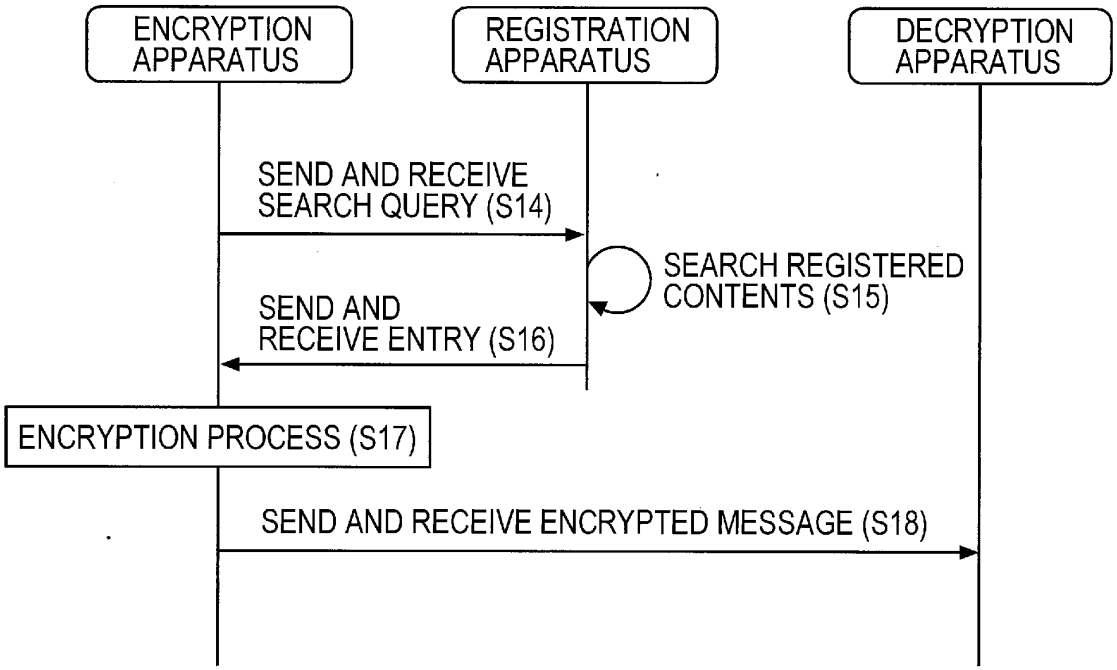

ENCRYPTION APPARATUS
REGISTRATION APPARATUS
DECRYPTION APPARATUS
SEND AND RECEIVE SEARCH QUERY (S14)
SEARCH REGISTERED CONTENTS (S15)
SEND AND RECEIVE ENTRY (S16)
ENCRYPTION PROCESS (S17)
SEND AND RECEIVE ENCRYPTED MESSAGE (S18)

FIG.4

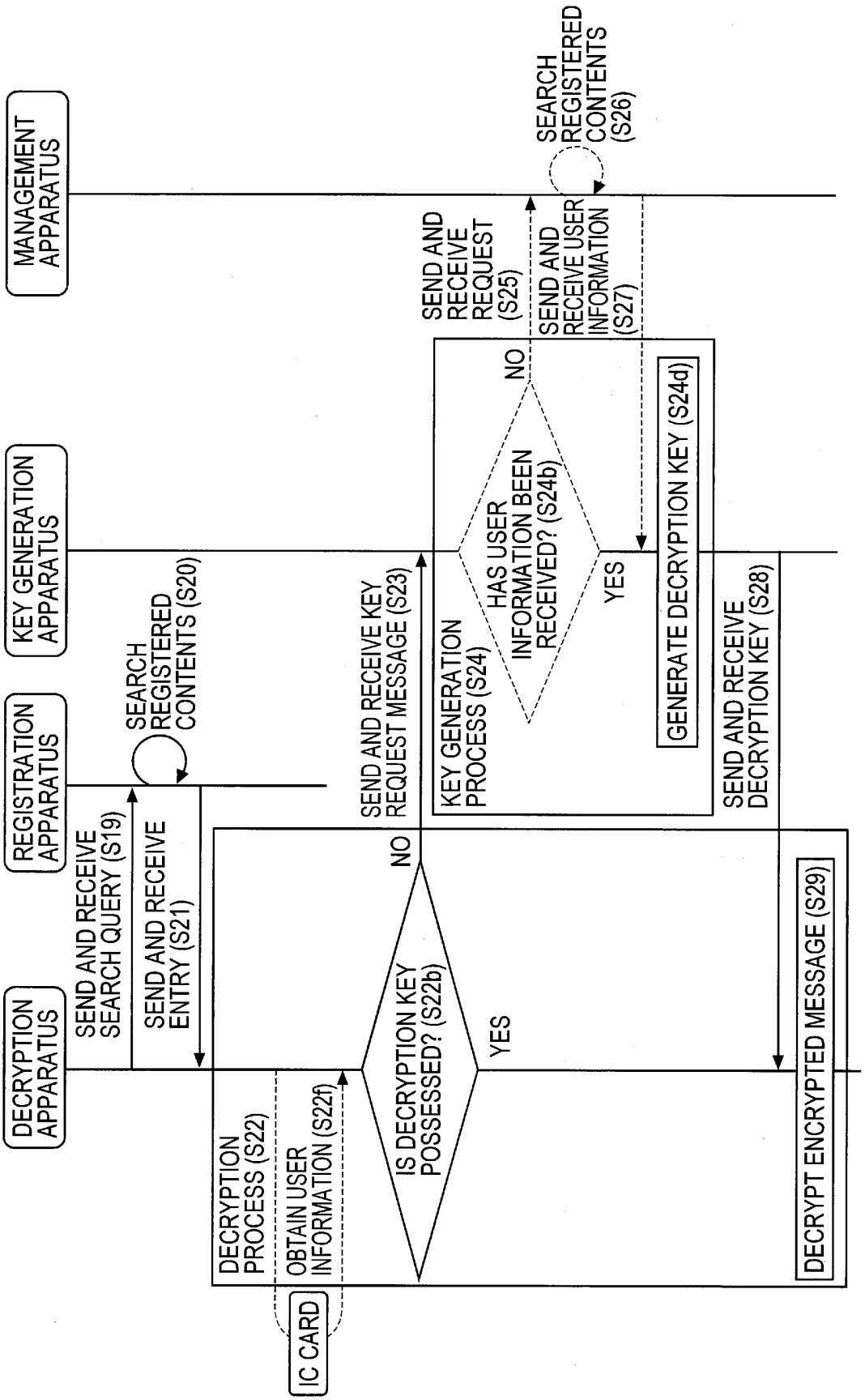

DECRYPTION APPARATUS
REGISTRATION APPARATUS
KEY GENERATION APPARATUS
MANAGEMENT APPARATUS
IC CARD
SEND AND RECEIVE SEARCH QUERY (S19)
SEND AND RECEIVE ENTRY (S21)
SEARCH REGISTERED CONTENTS (S20)
SEND AND RECEIVE KEY REQUEST MESSAGE (S23)
KEY GENERATION PROCESS (S24)
HAS USER INFORMATION BEEN RECEIVED? (S24b)
NO
YES
SEND AND RECEIVE REQUEST (S25)
SEARCH REGISTERED CONTENTS (S26)
SEND AND RECEIVE USER INFORMATION (S27)
GENERATE DECRYPTION KEY (S24d)
SEND AND RECEIVE DECRYPTION KEY (S28)
DECRYPTION PROCESS (S22)
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
DECRYPT ENCRYPTED MESSAGE (S29)

FIG.5

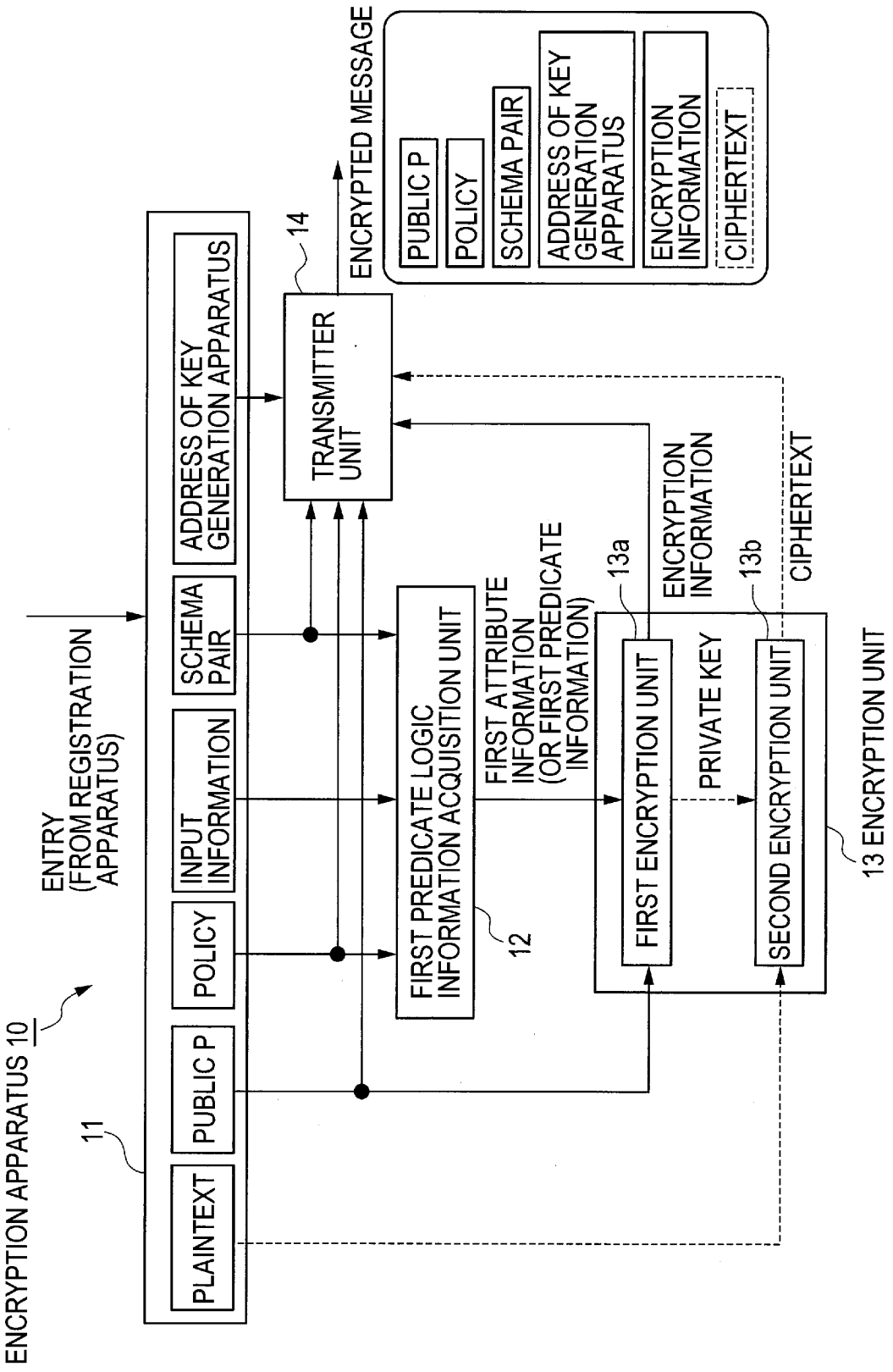

ENCRYPTION APPARATUS 10
11
ENTRY (FROM REGISTRATION APPARATUS)
PLAINTEXT
PUBLIC P
POLICY
INPUT INFORMATION
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
TRANSMITTER UNIT
14
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
CIPHERTEXT
FIRST PREDICATE LOGIC INFORMATION ACQUISITION UNIT
12
FIRST ATTRIBUTE INFORMATION (OR FIRST PREDICATE INFORMATION)
13a
FIRST ENCRYPTION UNIT
ENCRYPTION INFORMATION
PRIVATE KEY
13b
SECOND ENCRYPTION UNIT
CIPHERTEXT
13 ENCRYPTION UNIT

FIG.6

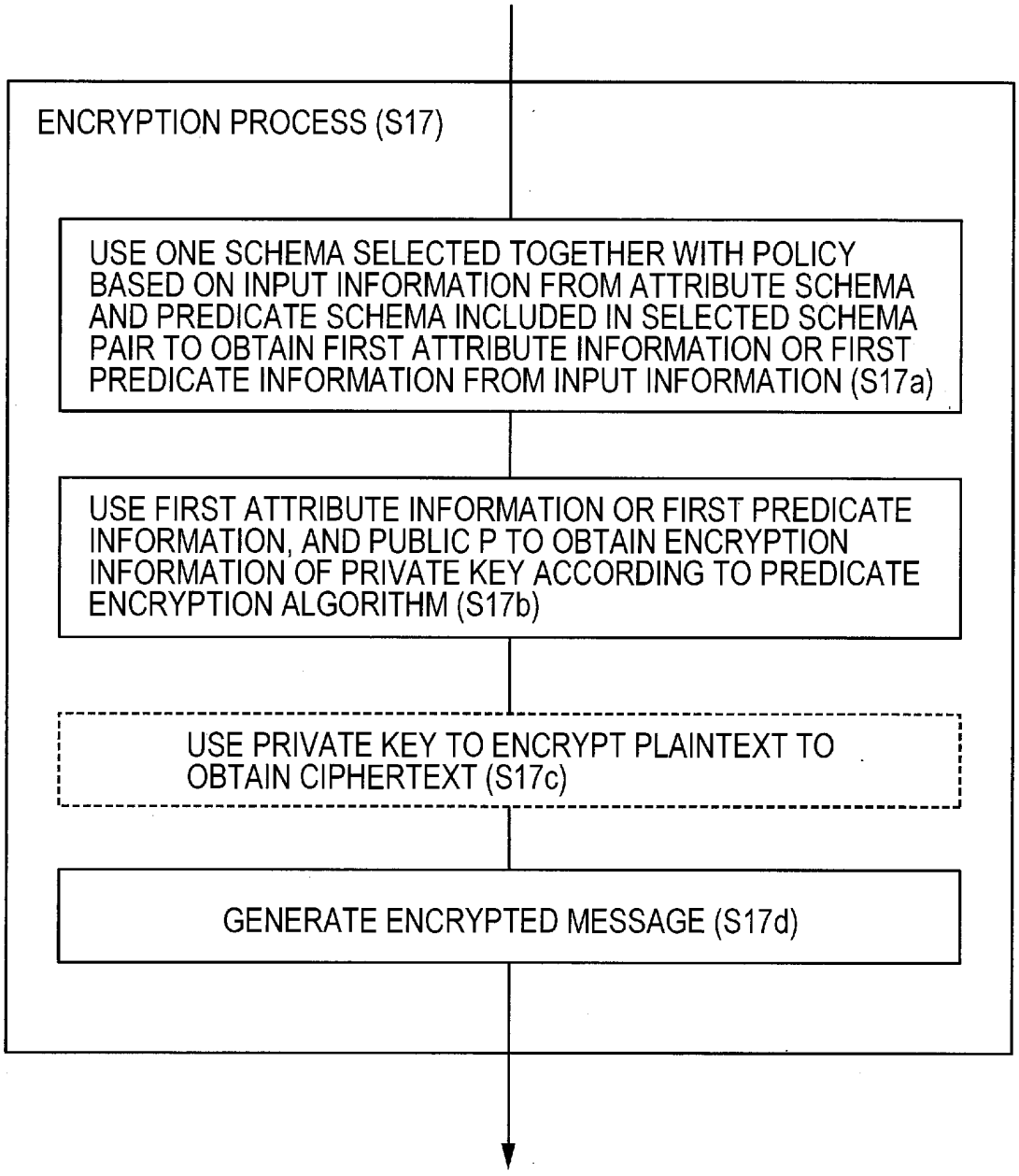

ENCRYPTION PROCESS (S17)
USE ONE SCHEMA SELECTED TOGETHER WITH POLICY BASED ON INPUT INFORMATION FROM ATTRIBUTE SCHEMA AND PREDICATE SCHEMA INCLUDED IN SELECTED SCHEMA PAIR TO OBTAIN FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION FROM INPUT INFORMATION (S17a)
USE FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION, AND PUBLIC P TO OBTAIN ENCRYPTION INFORMATION OF PRIVATE KEY ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S17b)
USE PRIVATE KEY TO ENCRYPT PLAINTEXT TO OBTAIN CIPHERTEXT (S17c)
GENERATE ENCRYPTED MESSAGE (S17d)

FIG.7

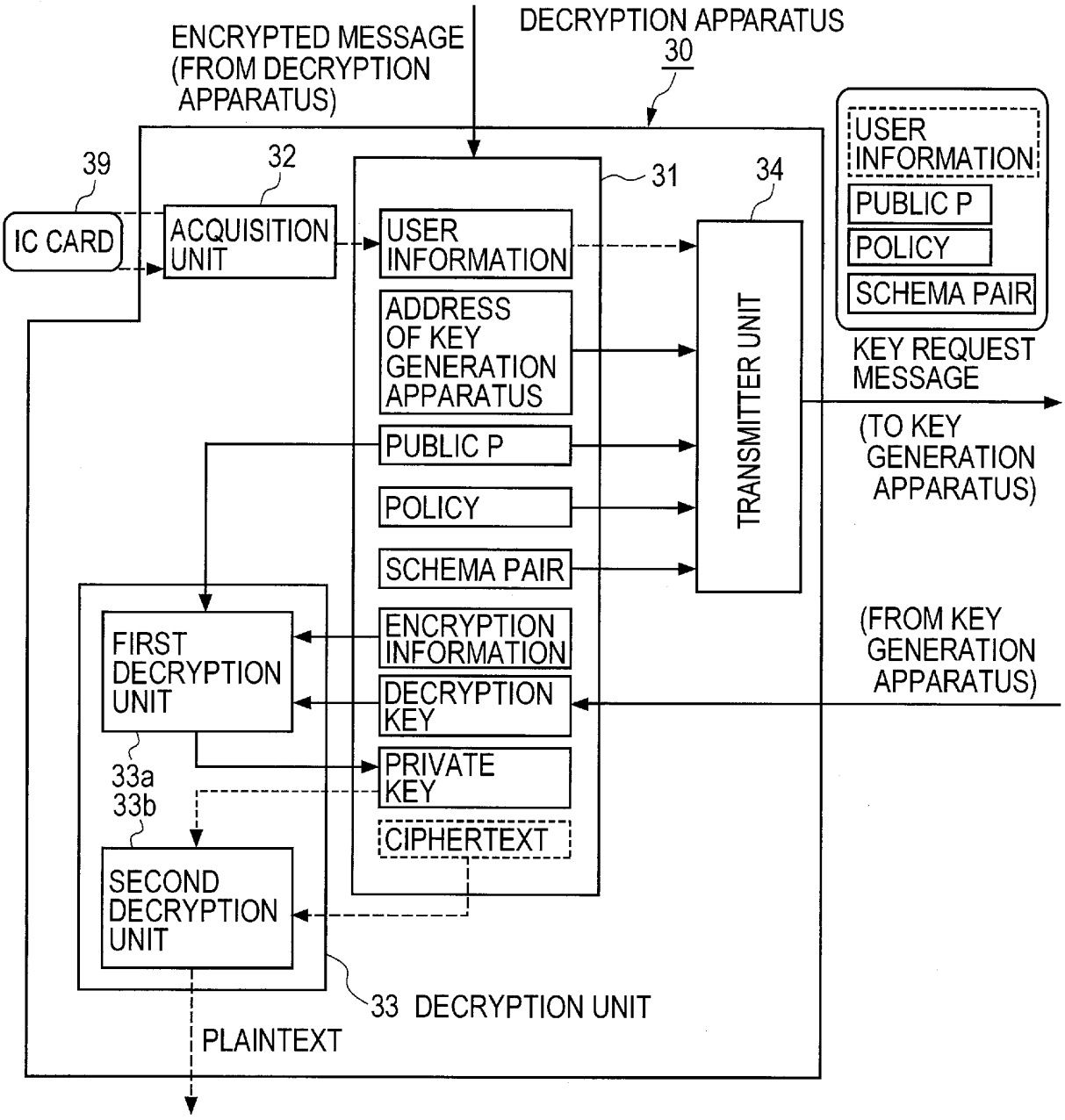

ENCRYPTED MESSAGE (FROM DECRYPTION APPARATUS)
DECRYPTION APPARATUS
30
39
32
31
34
IC CARD
ACQUISITION UNIT
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
(FROM KEY GENERATION APPARATUS)
FIRST DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
PRIVATE KEY
CIPHERTEXT
33a
33b
SECOND DECRYPTION UNIT
33 DECRYPTION UNIT
PLAINTEXT

FIG.8

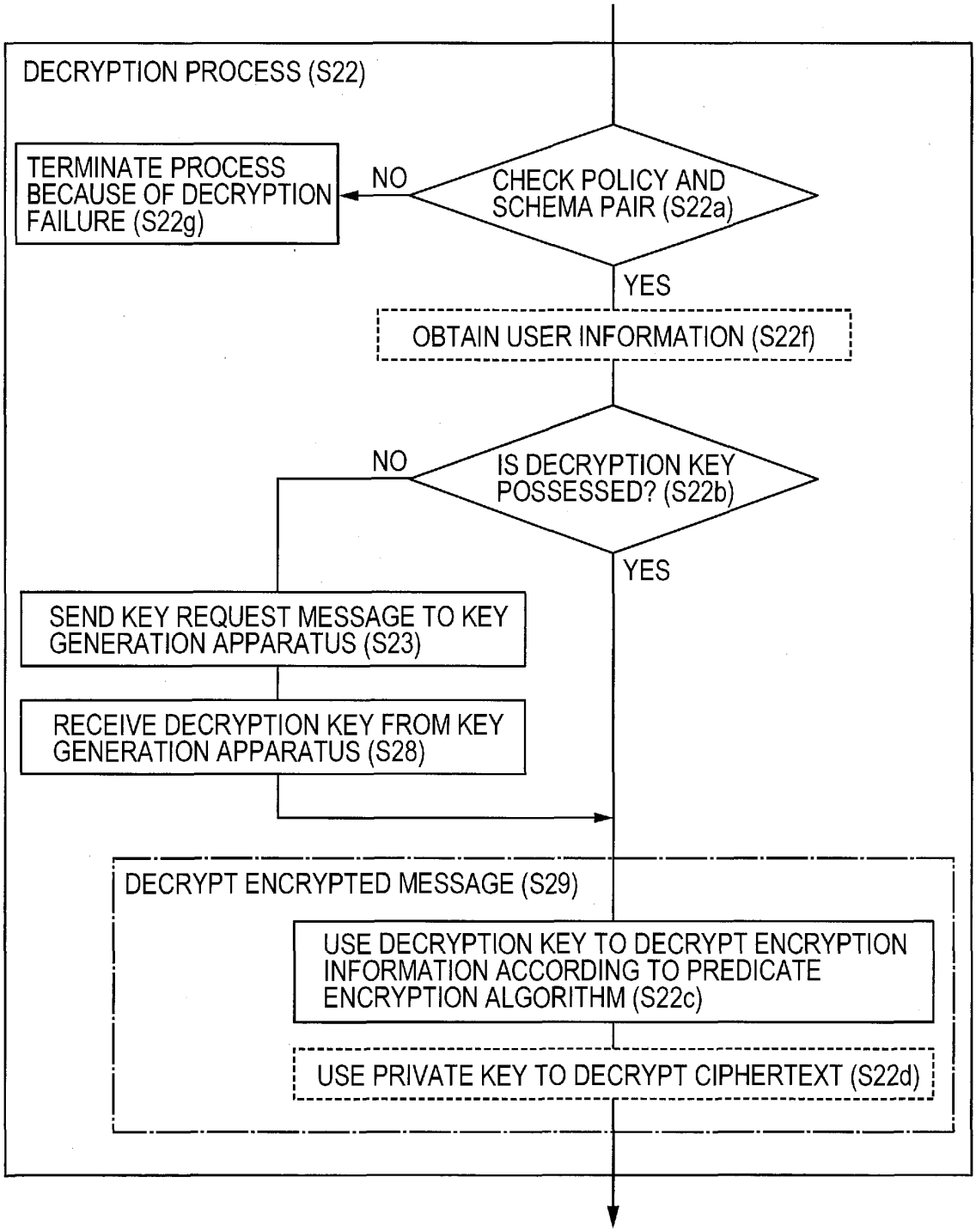

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c)
USE PRIVATE KEY TO DECRYPT CIPHERTEXT (S22d)

FIG.9

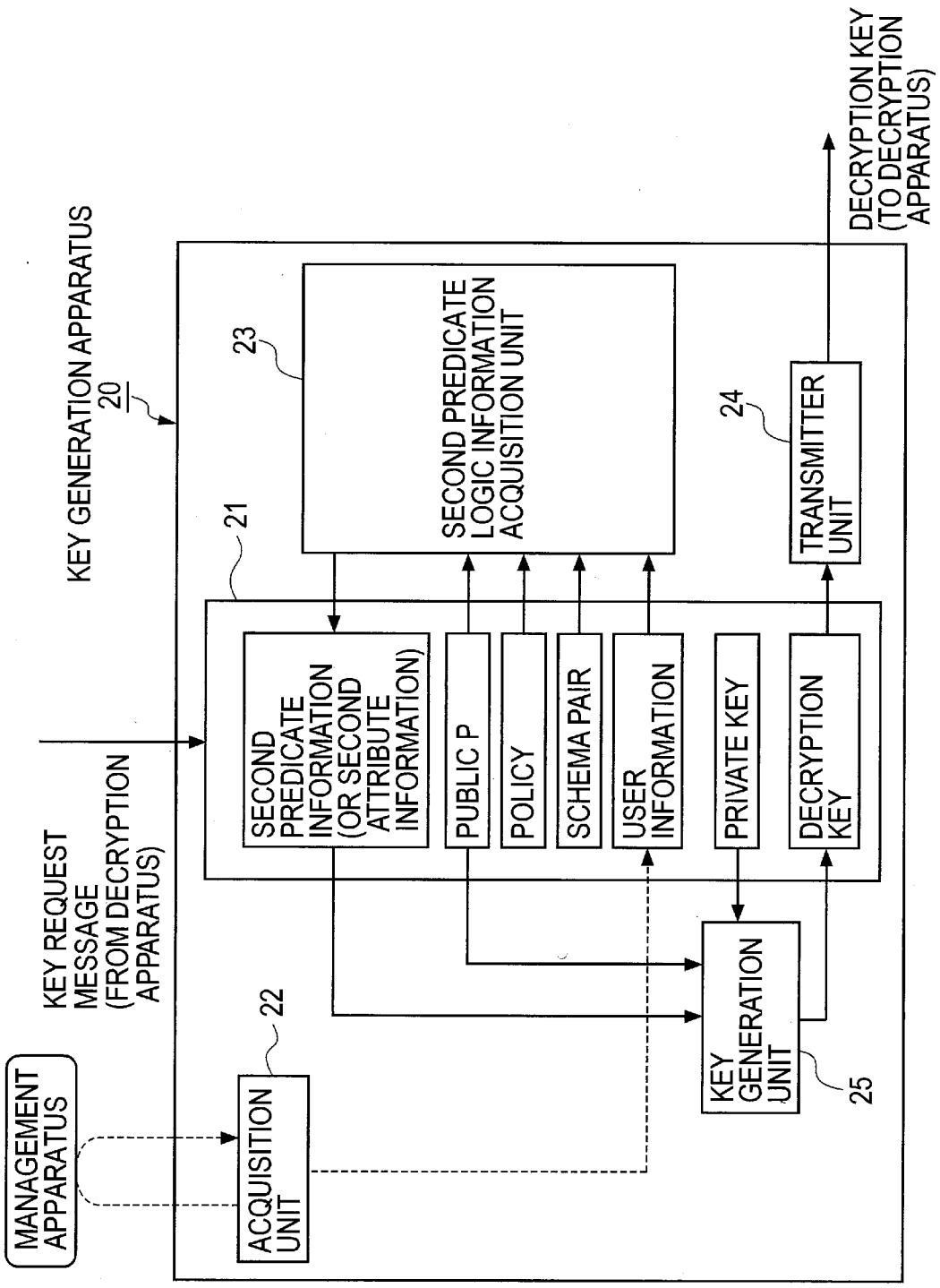

MANAGEMENT APPARATUS
KEY REQUEST MESSAGE (FROM DECRYPTION APPARATUS)
KEY GENERATION APPARATUS
20
ACQUISITION UNIT
22
21
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
PRIVATE KEY
DECRYPTION KEY
23
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
24
TRANSMITTER UNIT
KEY GENERATION UNIT
25
DECRYPTION KEY (TO DECRYPTION APPARATUS)

FIG.10

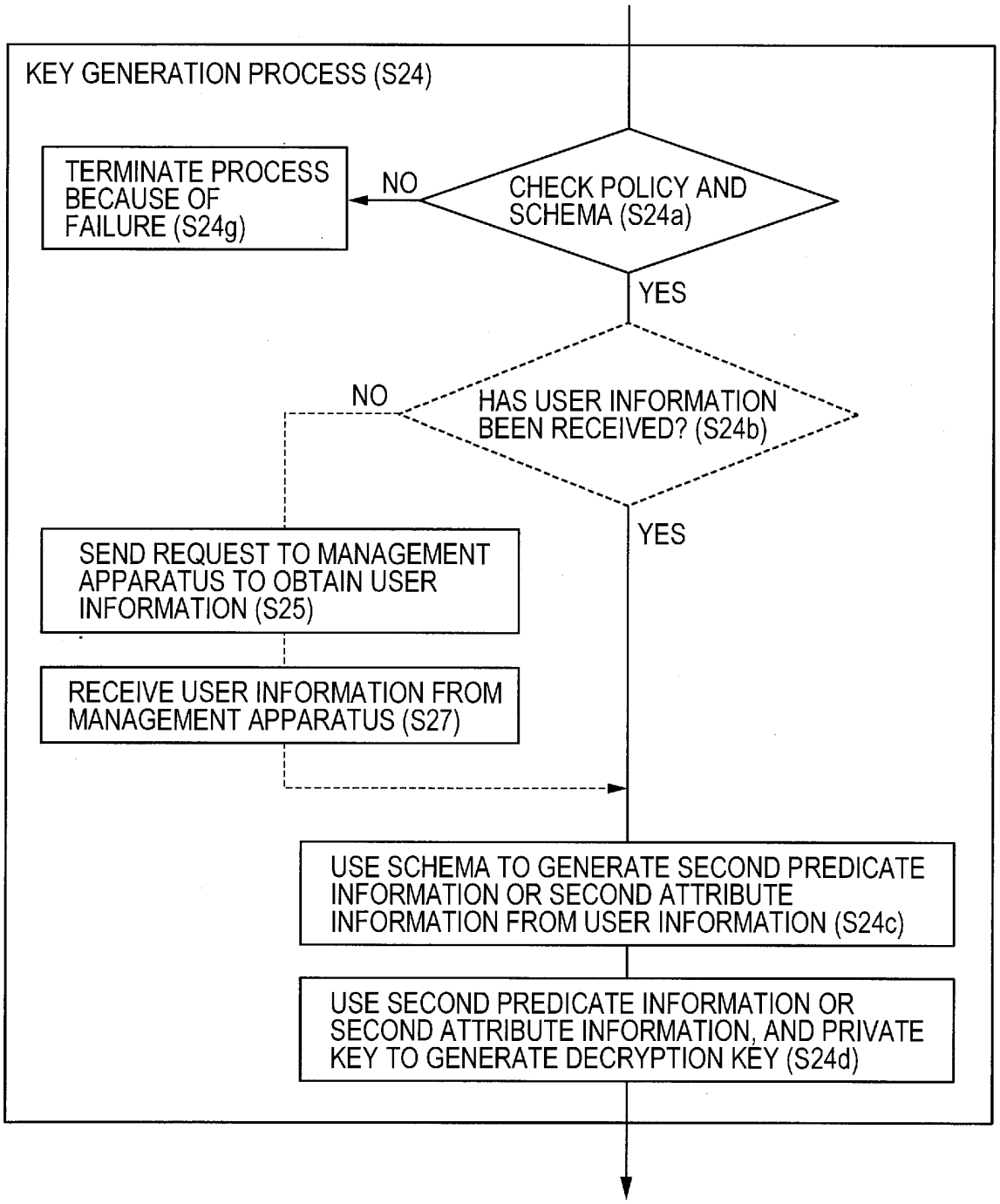

KEY GENERATION PROCESS (S24)
CHECK POLICY AND SCHEMA (S24a)
NO
TERMINATE PROCESS BECAUSE OF FAILURE (S24g)
YES
HAS USER INFORMATION BEEN RECEIVED? (S24b)
NO
YES
SEND REQUEST TO MANAGEMENT APPARATUS TO OBTAIN USER INFORMATION (S25)
RECEIVE USER INFORMATION FROM MANAGEMENT APPARATUS (S27)
USE SCHEMA TO GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION FROM USER INFORMATION (S24c)
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S24d)

FIG.11

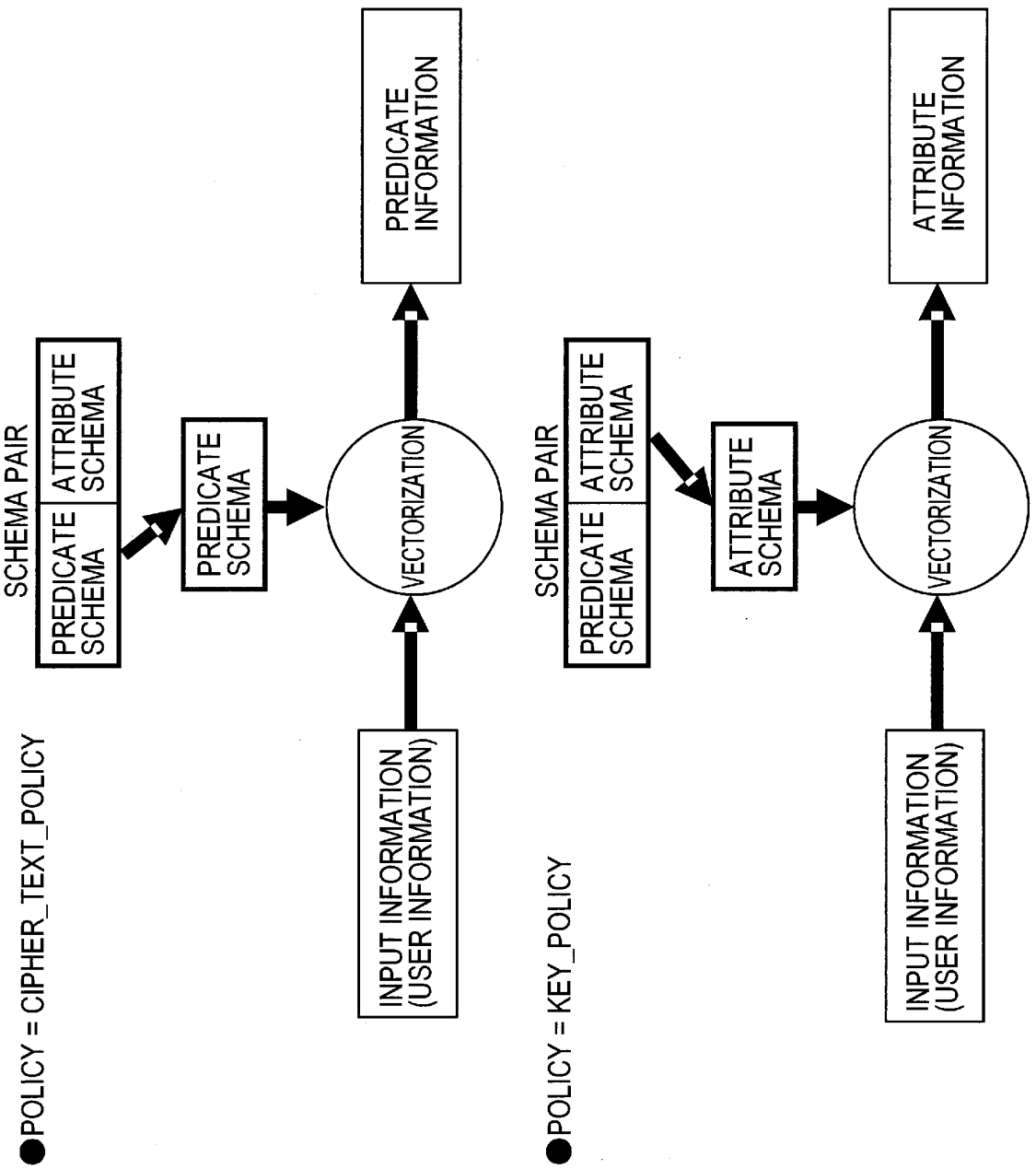

●POLICY = CIPHER_TEXT_POLICY
SCHEMA PAIR
PREDICATE SCHEMA
ATTRIBUTE SCHEMA
PREDICATE SCHEMA
VECTORIZATION
PREDICATE INFORMATION
INPUT INFORMATION (USER INFORMATION)
●POLICY = KEY_POLICY
SCHEMA PAIR
PREDICATE SCHEMA
ATTRIBUTE SCHEMA
ATTRIBUTE SCHEMA
VECTORIZATION
ATTRIBUTE INFORMATION
INPUT INFORMATION (USER INFORMATION)

FIG.12

EXAMPLE OF ATTRIBUTE SCHEMA

ELEMENT NUMBER	ATTRIBUTE NAME	TYPE CONVERSION FUNCTION
0	NAME	HASH FUNCTION
1	BLOOD TYPE	0 : 0 1 : A 2 : B 3 : AB
2,3	DATE OF BIRTH	ELEMENT 2: HASH(YEAR) ELEMENT 3: HASH(MONTH AND DAY)
4~104	AGE	VALUE OF ELEMENT X 1 : AGE > x -4 0 : AGE =< x -4

EXAMPLE OF USER ATTRIBUTE DESIGNATION INFORMATION

ATTRIBUTE NAME	DATA TYPE	ATTRIBUTE VALUE
NAME	CHARACTER STRING	TARO TANAKA IN KANJI
READING	CHARACTER STRING	TARO TANAKA
ADDRESS	ADDRESS	X-X-X, MIDORI-CHO, MUSASHINO, TOKYO
TELEPHONE NUMBER 1	TELEPHONE	0422-59-XXXX
FAX NUMBER 1	TELEPHONE	0422-59-XXXX
MOBILE PHONE NUMBER 1	TELEPHONE	090-XXXX-XXXX
MOBILE PHONE NUMBER 2	TELEPHONE	090-XXXX-XXXX
email1	CHARACTER STRING	XXX@XXX.ntt.co.jp
email2	CHARACTER STRING	XXX@XXX.ne.jp
DATA OF BIRTH	DATE	19XX/YY/ZZ
AGE	INTEGER	20
BLOOD TYPE	LIST	AB
. . .		

VECTORIZATION

EXAMPLE OF ATTRIBUTE INFORMATION (VECTOR INFORMATION)

ELEMENT NUMBER	ATTRIBUTE NAME	DATA TYPE	VALUE
0	NAME	CHARACTER STRING	HASH (TARO TANAKA IN KANJI)
1	BLOOD TYPE	LIST	3
2 3	DATA OF BIRTH	DATA	HASH(19XX) HASH(YY/ZZ)
4	AGE	INTEGER	1
5			1
...			...
23			1
24			0
...			...
104			0

EP 2 582 086 A1

FIG.13

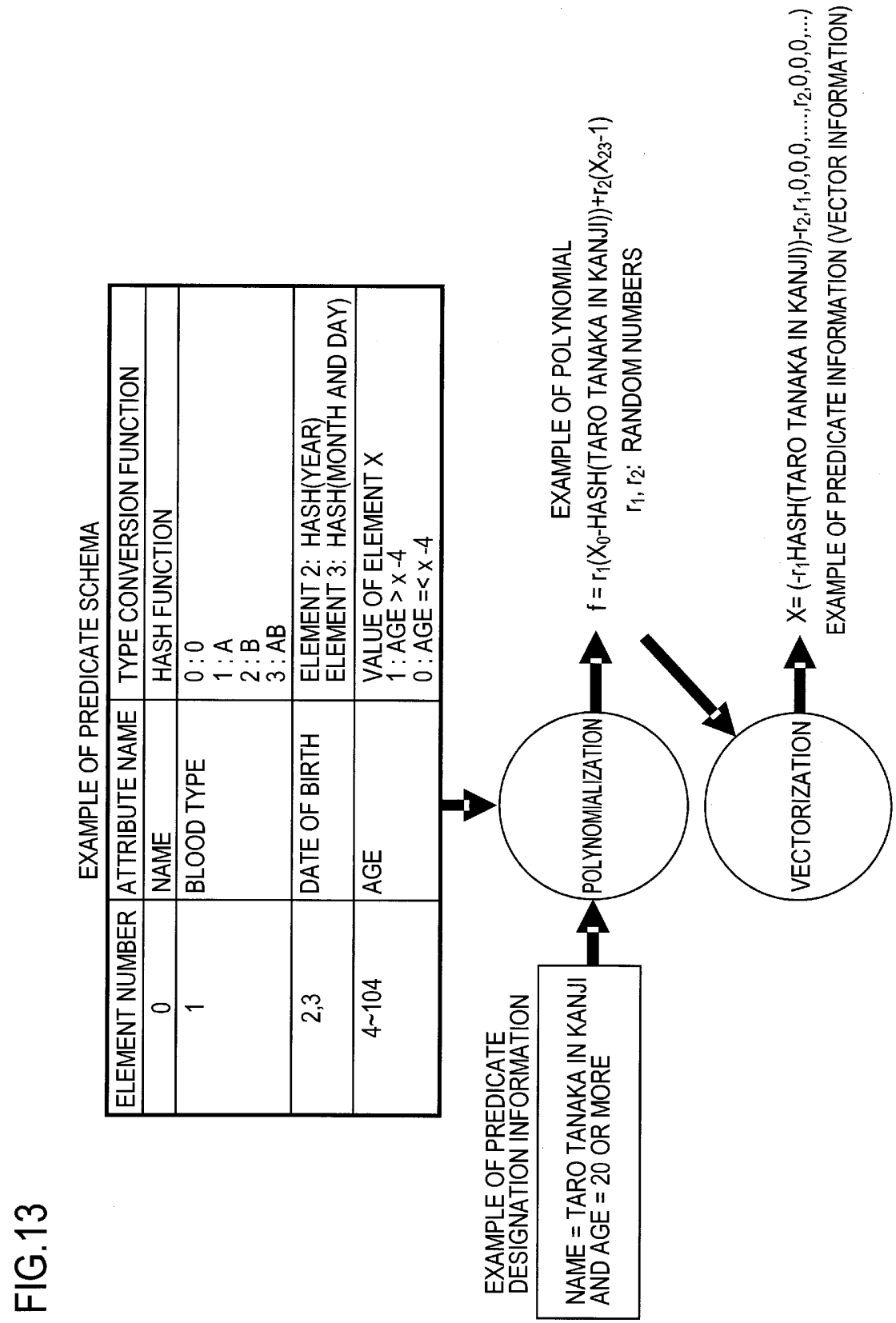

EXAMPLE OF PREDICATE SCHEMA
ELEMENT NUMBER
ATTRIBUTE NAME
TYPE CONVERSION FUNCTION
0
NAME
HASH FUNCTION
1
BLOOD TYPE
0 : 0
1 : A
2 : B
3 : AB
2,3
DATE OF BIRTH
ELEMENT 2: HASH(YEAR)
ELEMENT 3: HASH(MONTH AND DAY)
4~104
AGE
VALUE OF ELEMENT X
1 : AGE > x -4
0 : AGE =< x -4
EXAMPLE OF PREDICATE DESIGNATION INFORMATION
NAME = TARO TANAKA IN KANJI AND AGE = 20 OR MORE
POLYNOMIALIZATION
EXAMPLE OF POLYNOMIAL
f = r1(X0-HASH(TARO TANAKA IN KANJI))+r2(X23-1)
r1, r2: RANDOM NUMBERS
VECTORIZATION
X= (-r1HASH(TARO TANAKA IN KANJI))-r2,r1,0,0,0,...,r2,0,0,0,...)
EXAMPLE OF PREDICATE INFORMATION (VECTOR INFORMATION)

FIG.14

EXAMPLE: POLICY LIST LIMITED TO CIPHER_TEXT_POLICY

ITEM NUMBER	POLICY
1	CIPHER_TEXT_POLICY

EXAMPLE: POLICY LIST LIMITED TO KEY_POLICY

ITEM NUMBER	POLICY
1	KEY_POLICY

EXAMPLE: POLICY LIST FOR CIPHER_TEXT_POLICY AND KEY_POLICY

ITEM NUMBER	POLICY
1	CIPHER_TEXT_POLICY
2	KEY_POLICY

FIG.15

IDENTIFIER OF KEY GENERATION APPARATUS	PUBLIC PARAMETER	SCHEMA PAIR	DECRYPTION KEY TARGET	PREDICATE DESIGNATION INFORMATION	DECRYPTION KEY
KEY GENERATION APPARATUS 20-1	PUBLIC PARAMETER 1	SCHEMA PAIR 1			DECRYPTION KEY 1
KEY GENERATION APPARATUS 20-2	PUBLIC PARAMETER 2	SCHEMA PAIR 2			DECRYPTION KEY 2
. . .	. . .	. . .			. . .
KEY GENERATION APPARATUS 20-N	PUBLIC PARAMETER N	SCHEMA PAIR N			DECRYPTION KEY N

EP 2 582 086 A1

FIG.16

USER ID	PASSWORD
USER 1	PASSWORD 1
USER 2	PASSWORD 2
. . .	. . .
USER N	PASSWORD N

FIG.17

USER ID	ATTRIBUTE NAME	ATTRIBUTE VALUE
USER 1	ATTRIBUTE NAME 1	ATTRIBUTE VALUE 1
USER 1	ATTRIBUTE NAME 2	ATTRIBUTE VALUE 2
...	...	...
USER 1	ATTRIBUTE NAME N	ATTRIBUTE VALUE N
...	...	...
USER M	ATTRIBUTE NAME K	ATTRIBUTE VALUE K
...	...	...

USER ID	PREDICATE
USER 1	PREDICATE 1
USER 2	PREDICATE 2
...	...
USER N	PREDICATE N

FIG.18

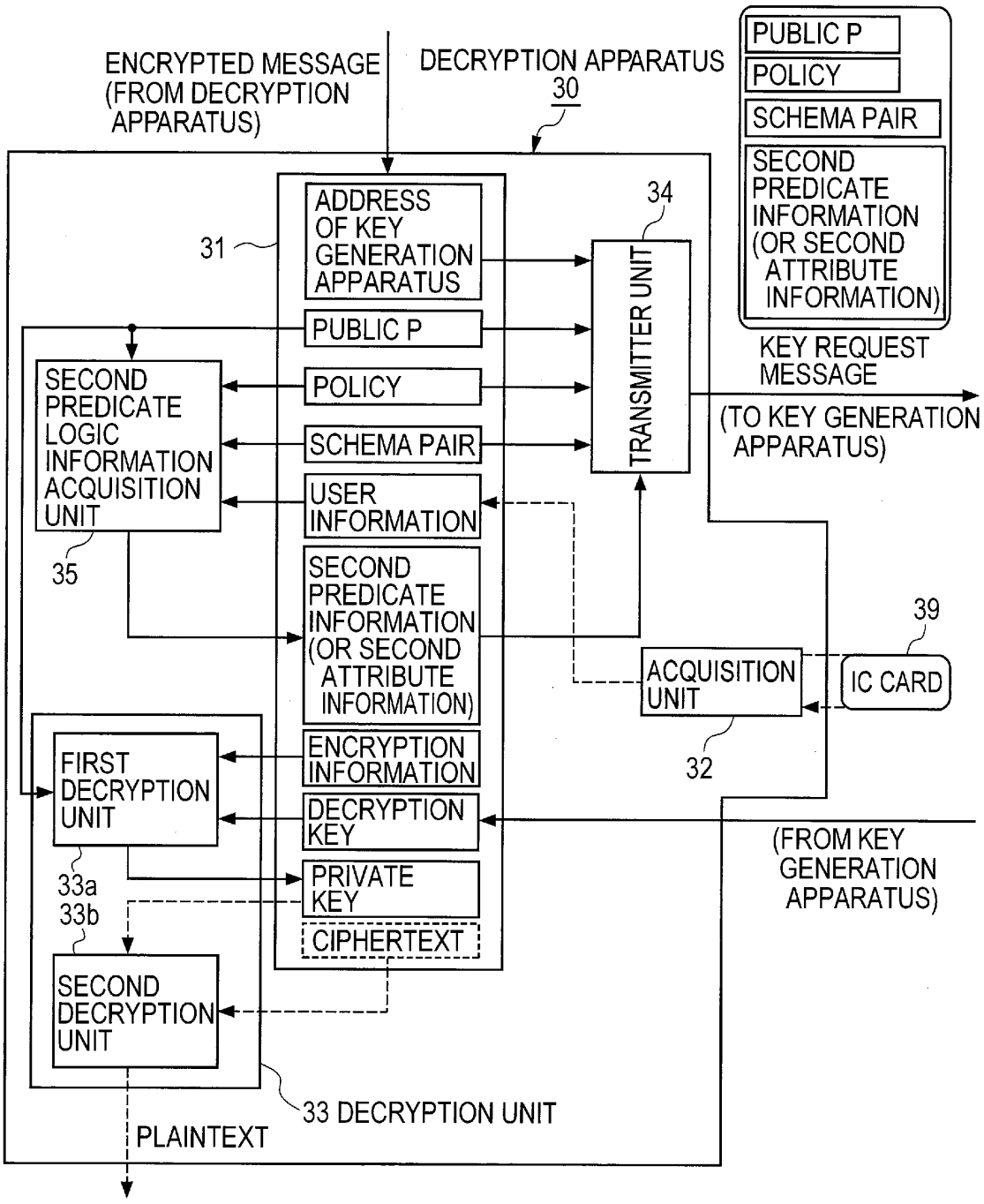

ENCRYPTED MESSAGE (FROM DECRYPTION APPARATUS)
DECRYPTION APPARATUS
30
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
31
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
ENCRYPTION INFORMATION
DECRYPTION KEY
PRIVATE KEY
CIPHERTEXT
34
TRANSMITTER UNIT
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
39
ACQUISITION UNIT
IC CARD
32
FIRST DECRYPTION UNIT
33a
33b
SECOND DECRYPTION UNIT
33 DECRYPTION UNIT
(FROM KEY GENERATION APPARATUS)
PLAINTEXT

FIG.19

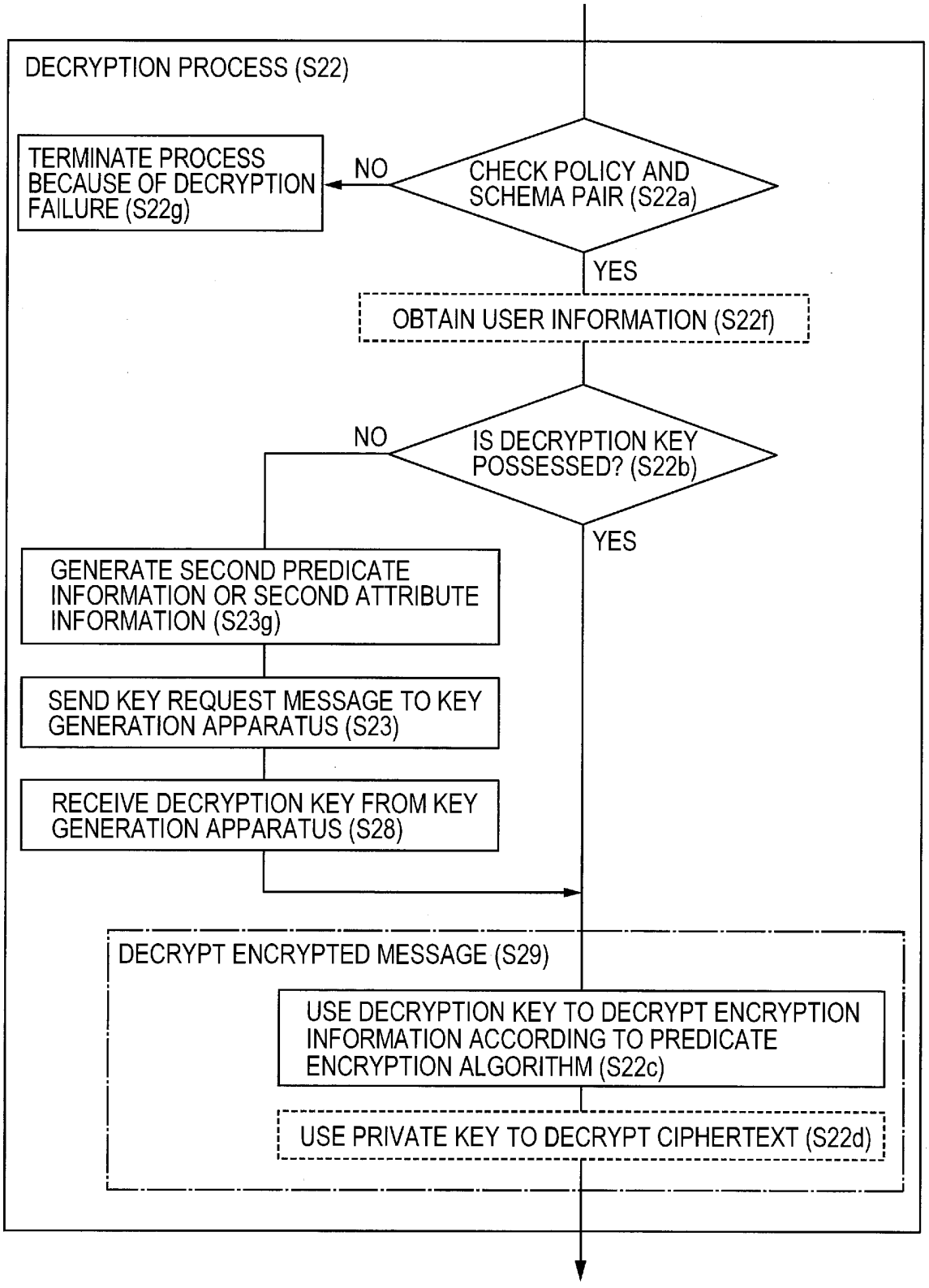

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S23g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c)
USE PRIVATE KEY TO DECRYPT CIPHERTEXT (S22d)

FIG.20

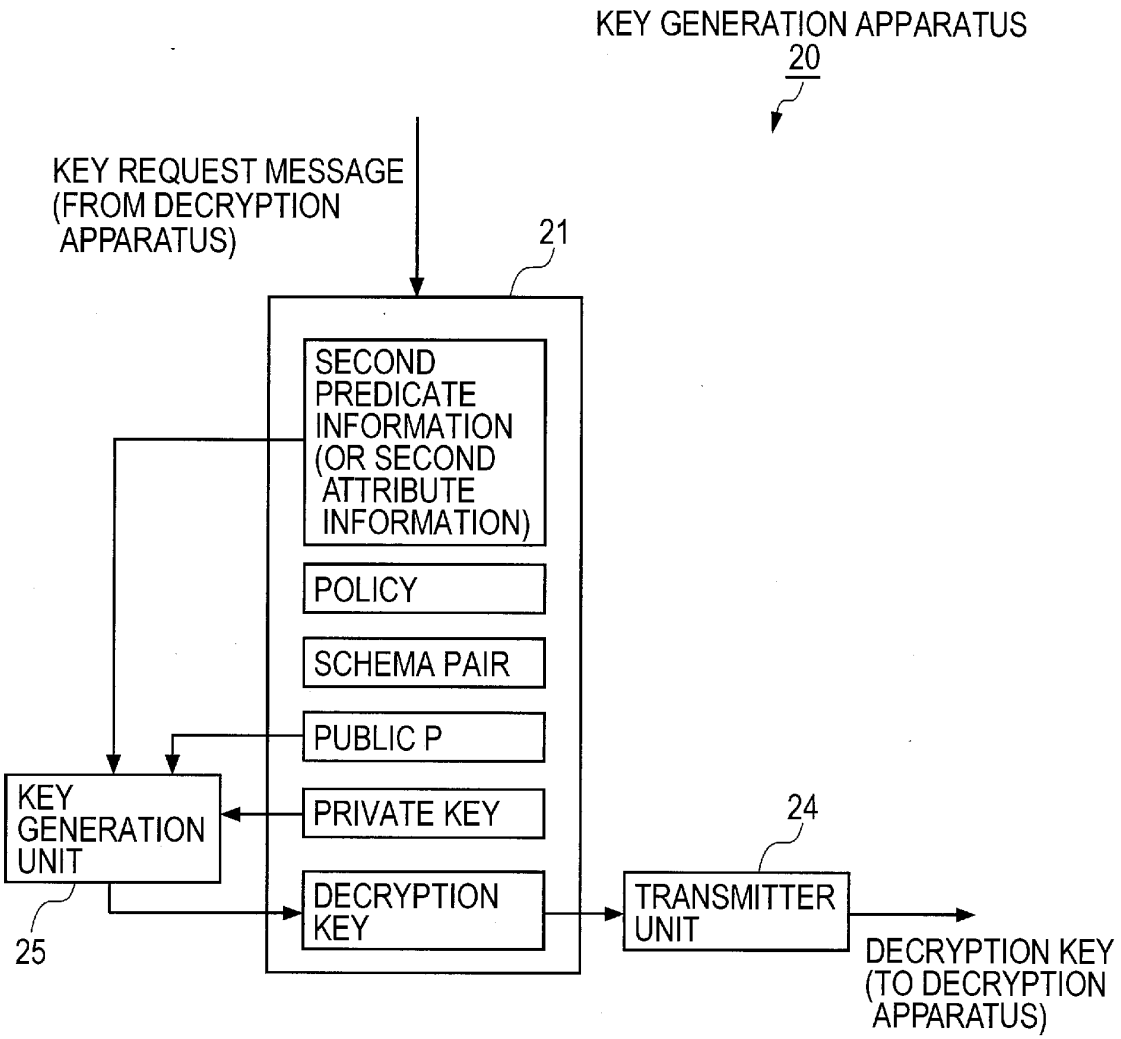

KEY GENERATION APPARATUS
20
KEY REQUEST MESSAGE (FROM DECRYPTION APPARATUS)
21
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
POLICY
SCHEMA PAIR
PUBLIC P
PRIVATE KEY
DECRYPTION KEY
KEY GENERATION UNIT
25
24
TRANSMITTER UNIT
DECRYPTION KEY (TO DECRYPTION APPARATUS)

FIG.21

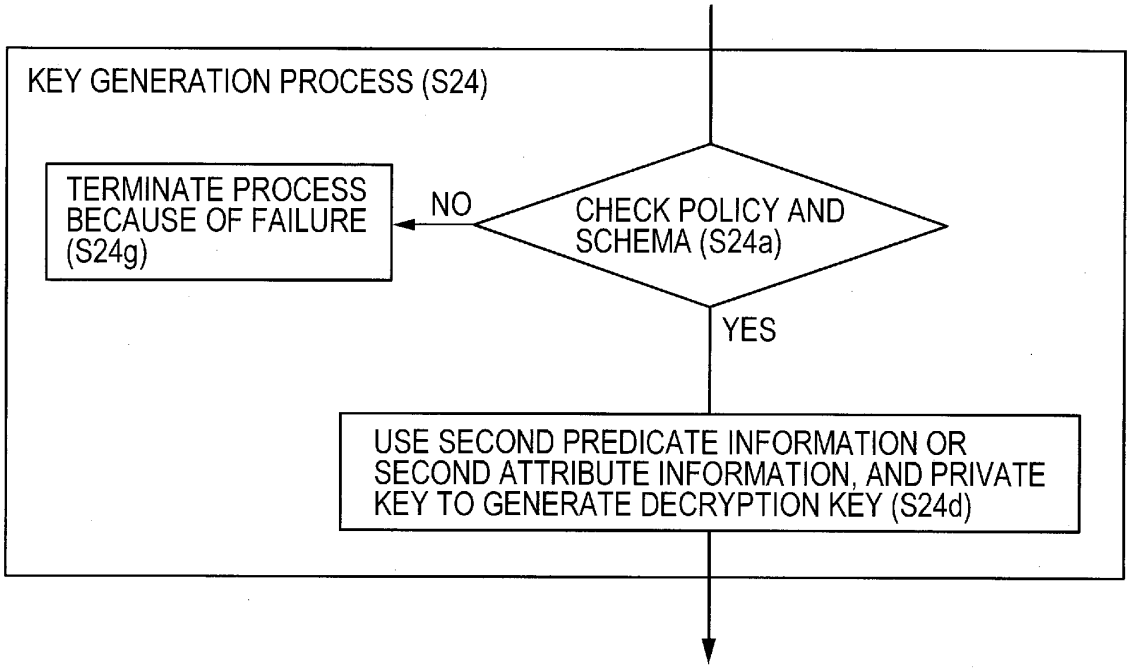

KEY GENERATION PROCESS (S24)
TERMINATE PROCESS BECAUSE OF FAILURE (S24g)
NO
CHECK POLICY AND SCHEMA (S24a)
YES
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S24d)

FIG.22

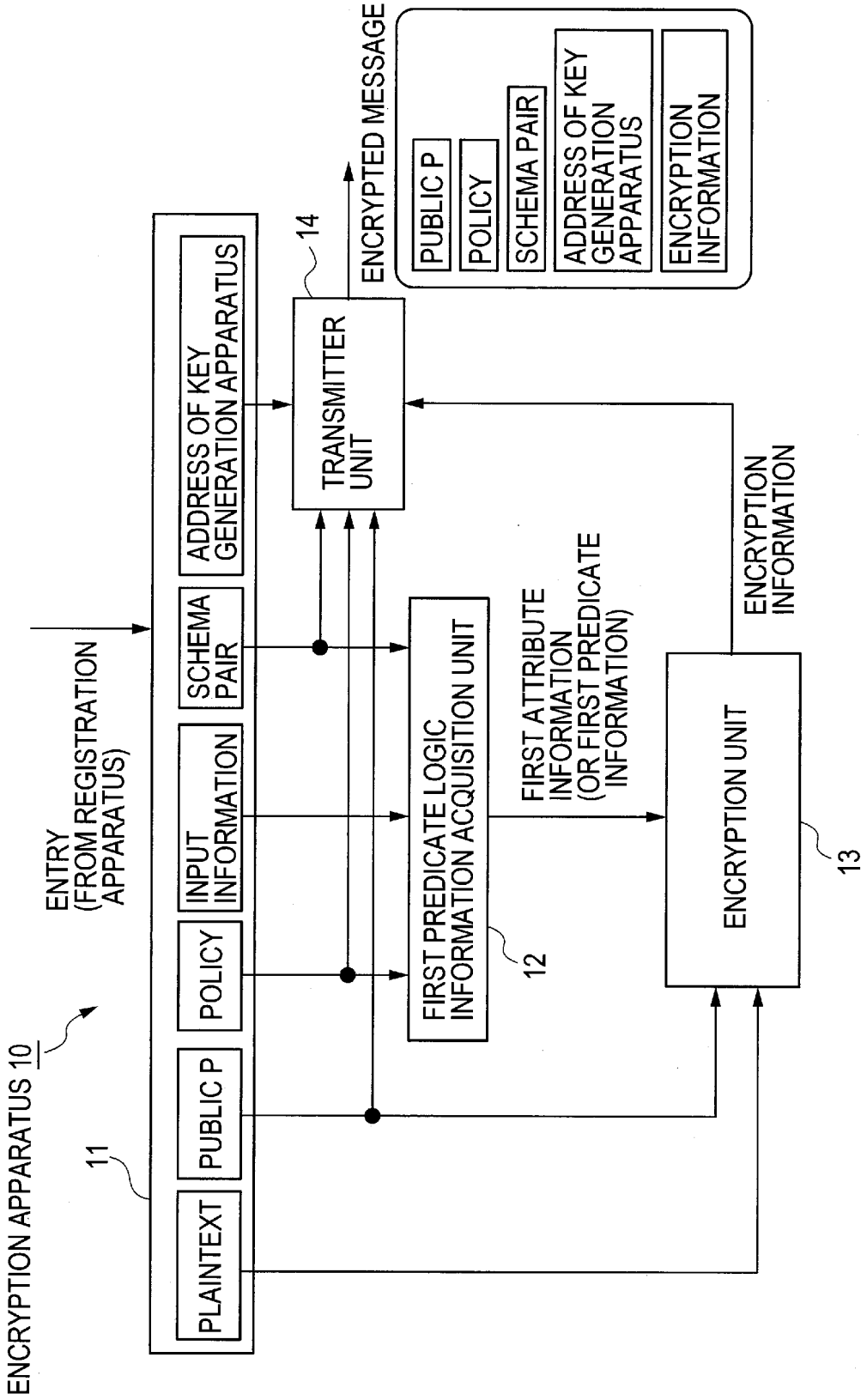

ENCRYPTION APPARATUS 10
11
ENTRY (FROM REGISTRATION APPARATUS)
PLAINTEXT
PUBLIC P
POLICY
INPUT INFORMATION
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
FIRST PREDICATE LOGIC INFORMATION ACQUISITION UNIT
12
TRANSMITTER UNIT
14
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
FIRST ATTRIBUTE INFORMATION (OR FIRST PREDICATE INFORMATION)
ENCRYPTION INFORMATION
ENCRYPTION UNIT
13

FIG.23

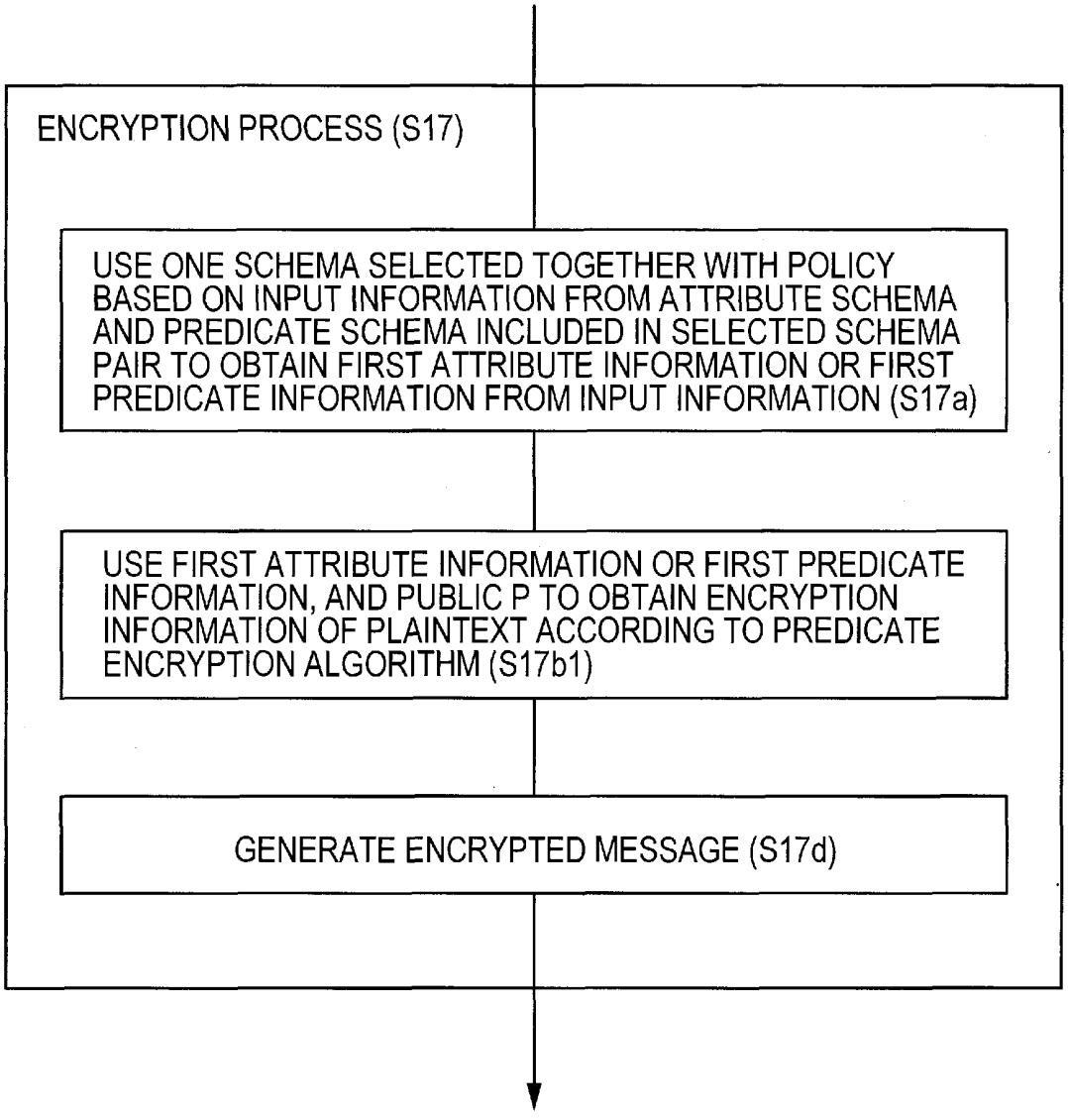

ENCRYPTION PROCESS (S17)
USE ONE SCHEMA SELECTED TOGETHER WITH POLICY BASED ON INPUT INFORMATION FROM ATTRIBUTE SCHEMA AND PREDICATE SCHEMA INCLUDED IN SELECTED SCHEMA PAIR TO OBTAIN FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION FROM INPUT INFORMATION (S17a)
USE FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION, AND PUBLIC P TO OBTAIN ENCRYPTION INFORMATION OF PLAINTEXT ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S17b1)
GENERATE ENCRYPTED MESSAGE (S17d)

FIG.24

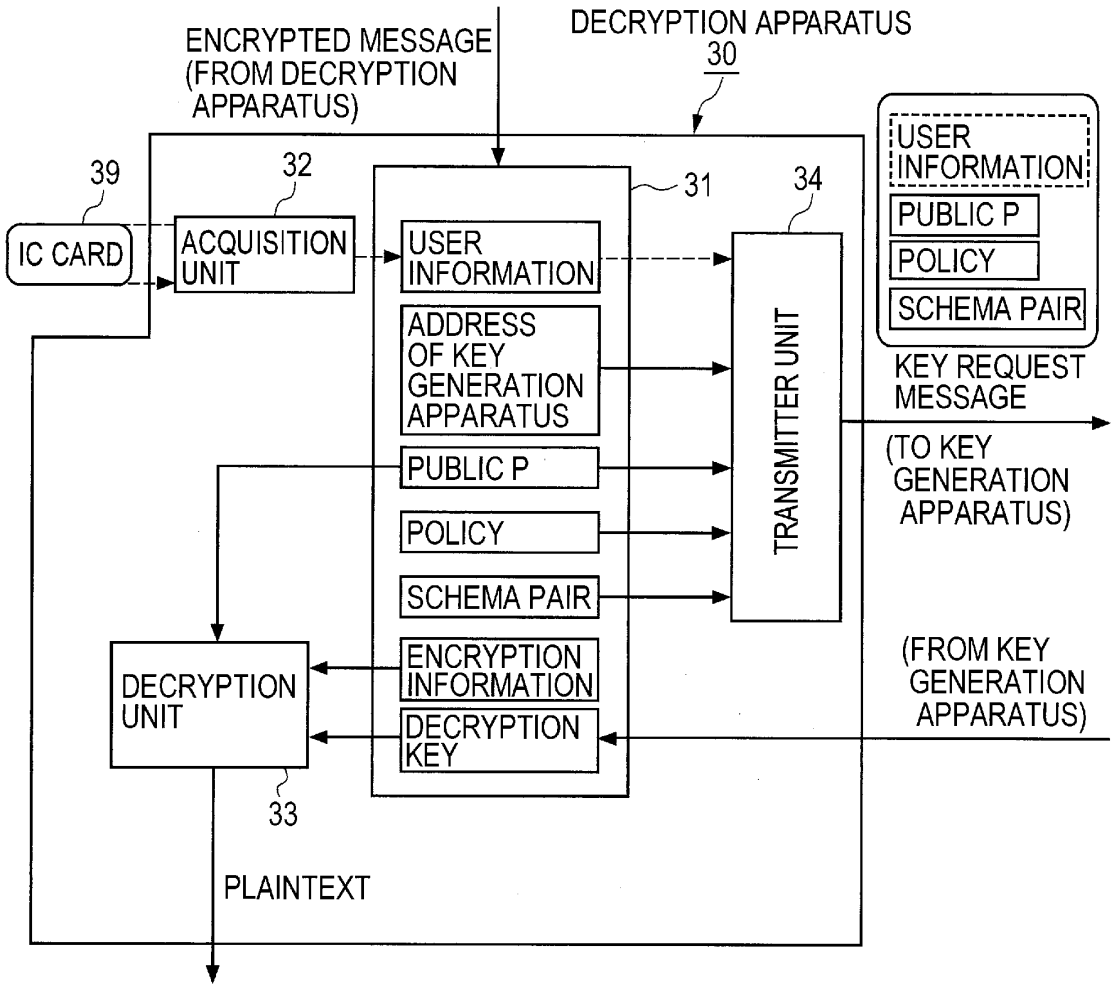

ENCRYPTED MESSAGE (FROM DECRYPTION APPARATUS)
DECRYPTION APPARATUS
30
39
32
31
34
IC CARD
ACQUISITION UNIT
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
(FROM KEY GENERATION APPARATUS)
33
PLAINTEXT

FIG.25

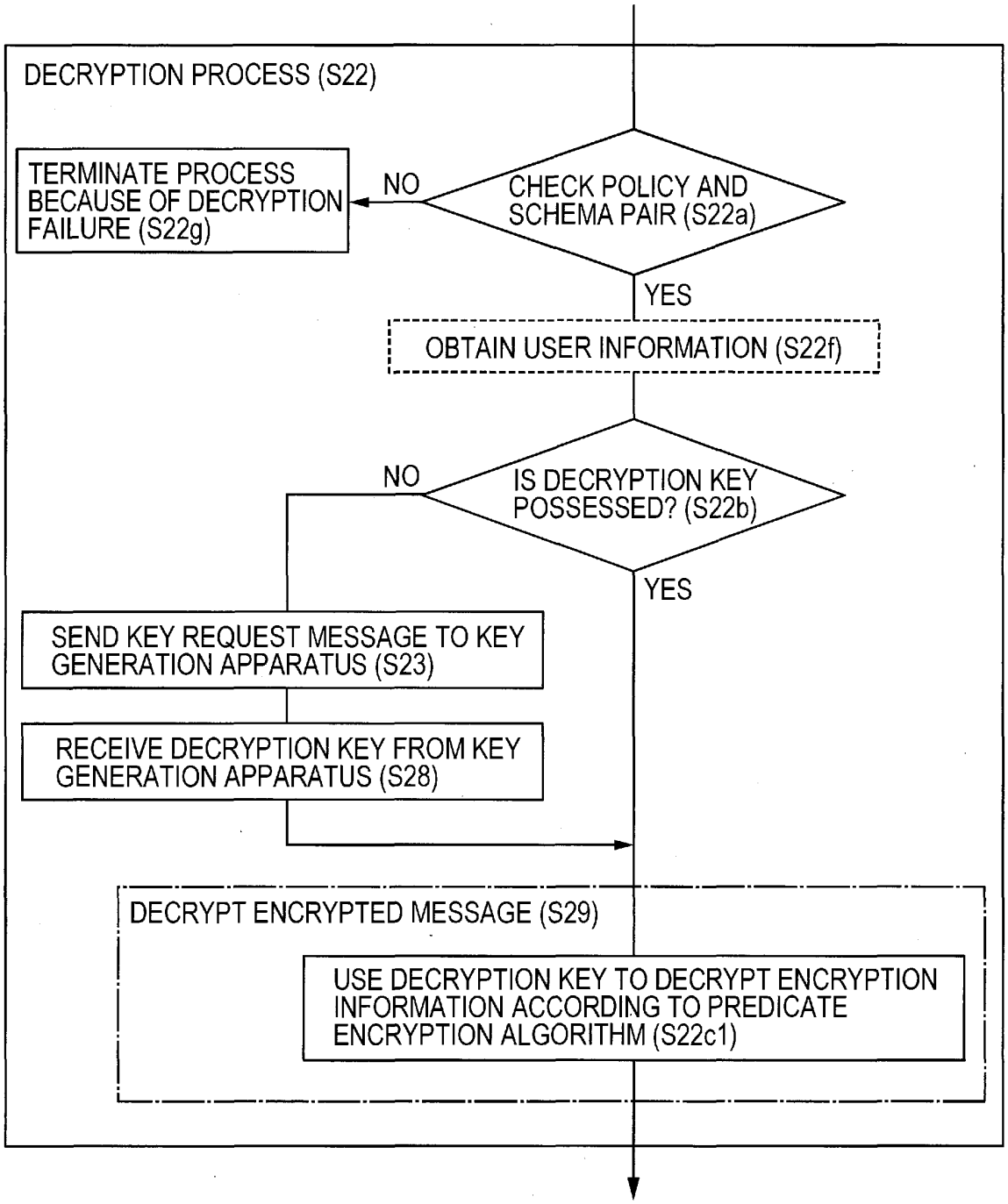

DECRYPTION PROCESS (S22)
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
NO
CHECK POLICY AND SCHEMA PAIR (S22a)
YES
OBTAIN USER INFORMATION (S22f)
NO
IS DECRYPTION KEY POSSESSED? (S22b)
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c1)

FIG.26

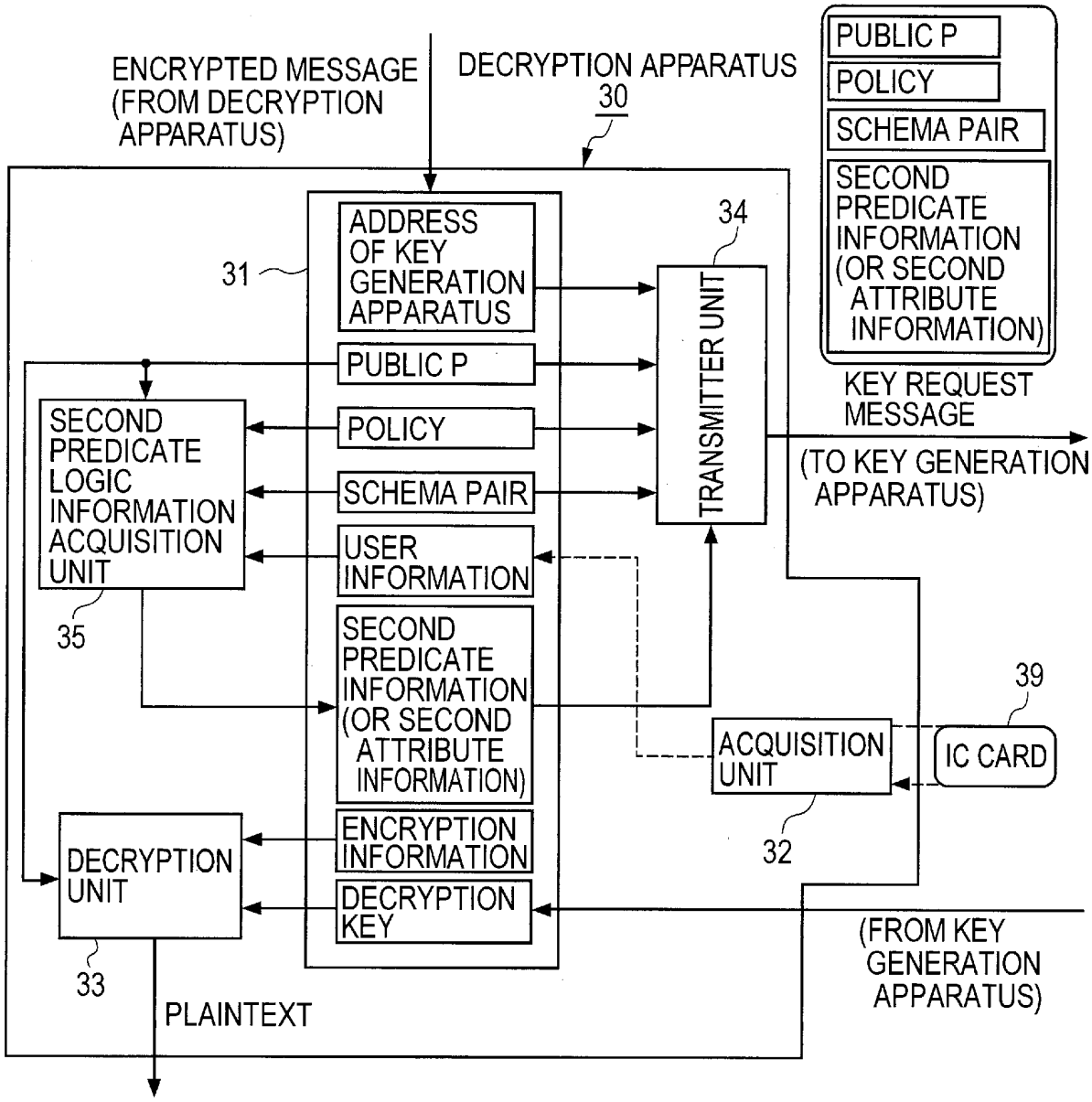

ENCRYPTED MESSAGE (FROM DECRYPTION APPARATUS)
DECRYPTION APPARATUS
30
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
31
ADDRESS OF KEY GENERATION APPARATUS
34
TRANSMITTER UNIT
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
ENCRYPTION INFORMATION
DECRYPTION KEY
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
39
ACQUISITION UNIT
IC CARD
32
DECRYPTION UNIT
33
PLAINTEXT
(FROM KEY GENERATION APPARATUS)

FIG.27

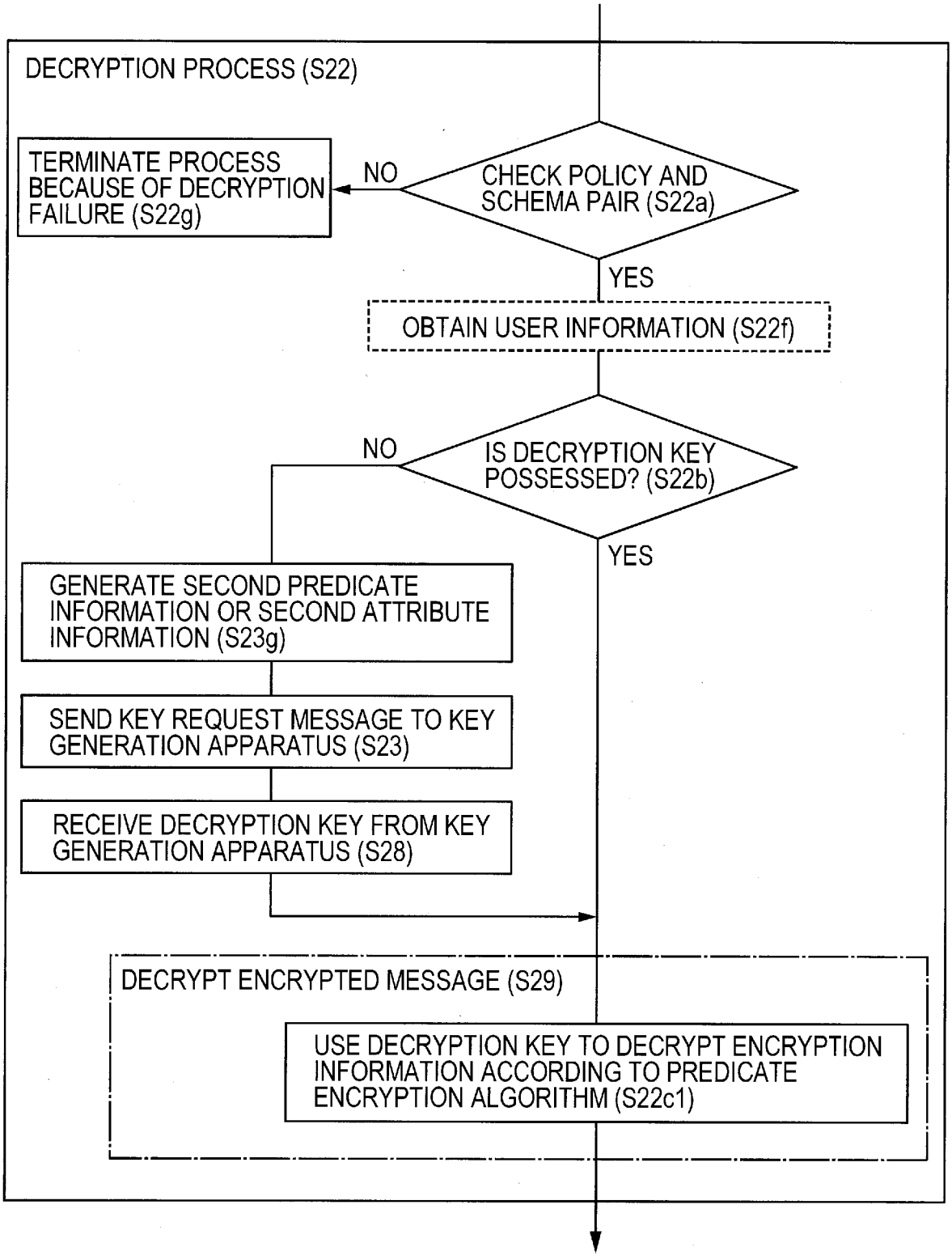

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S23g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c1)

FIG.28

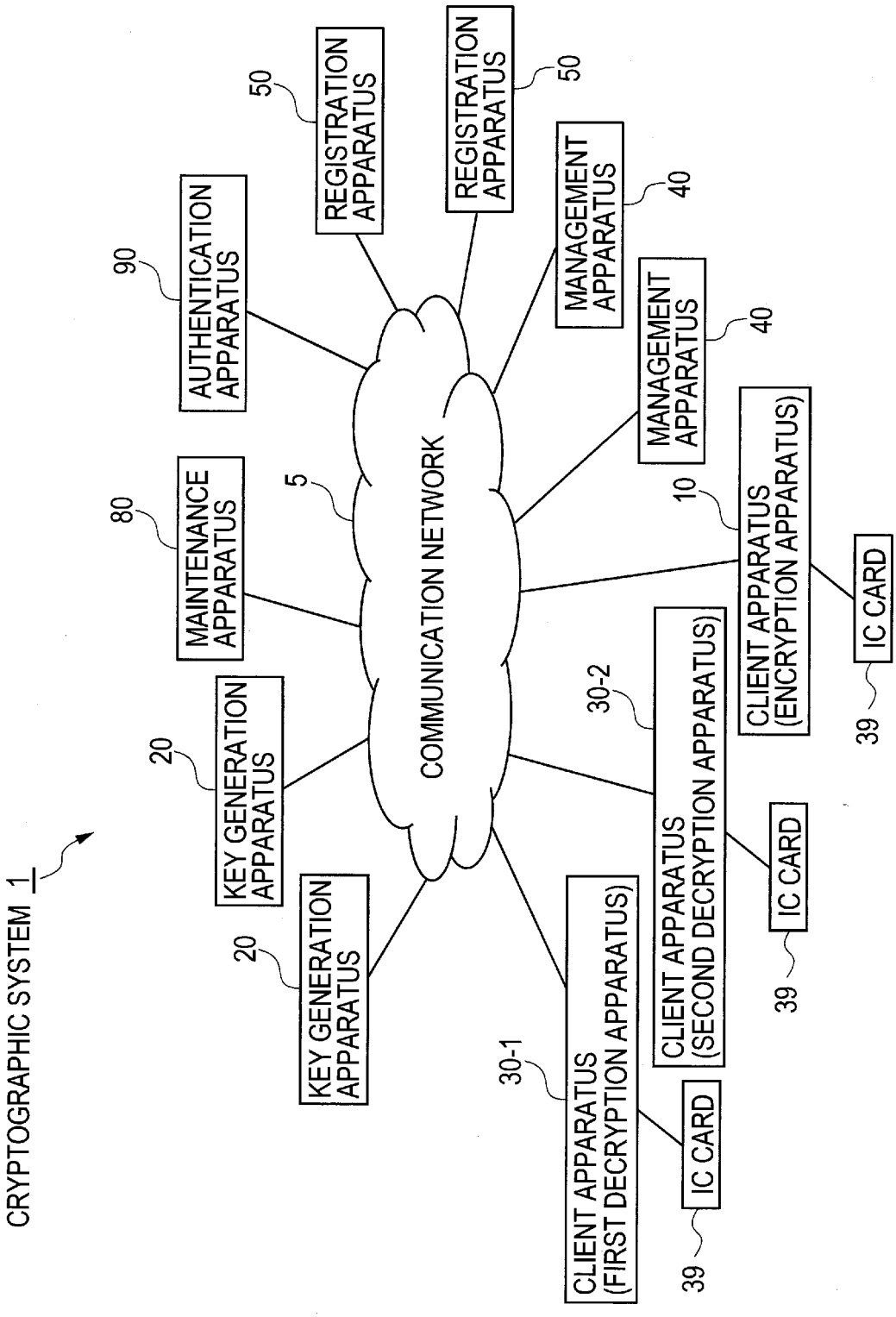

CRYPTOGRAPHIC SYSTEM 1
COMMUNICATION NETWORK
5
AUTHENTICATION APPARATUS
90
REGISTRATION APPARATUS
50
REGISTRATION APPARATUS
50
MANAGEMENT APPARATUS
40
MANAGEMENT APPARATUS
40
MAINTENANCE APPARATUS
80
KEY GENERATION APPARATUS
20
KEY GENERATION APPARATUS
20
CLIENT APPARATUS (ENCRYPTION APPARATUS)
10
IC CARD
39
CLIENT APPARATUS (SECOND DECRYPTION APPARATUS)
30-2
IC CARD
39
CLIENT APPARATUS (FIRST DECRYPTION APPARATUS)
30-1
IC CARD
39

FIG.29

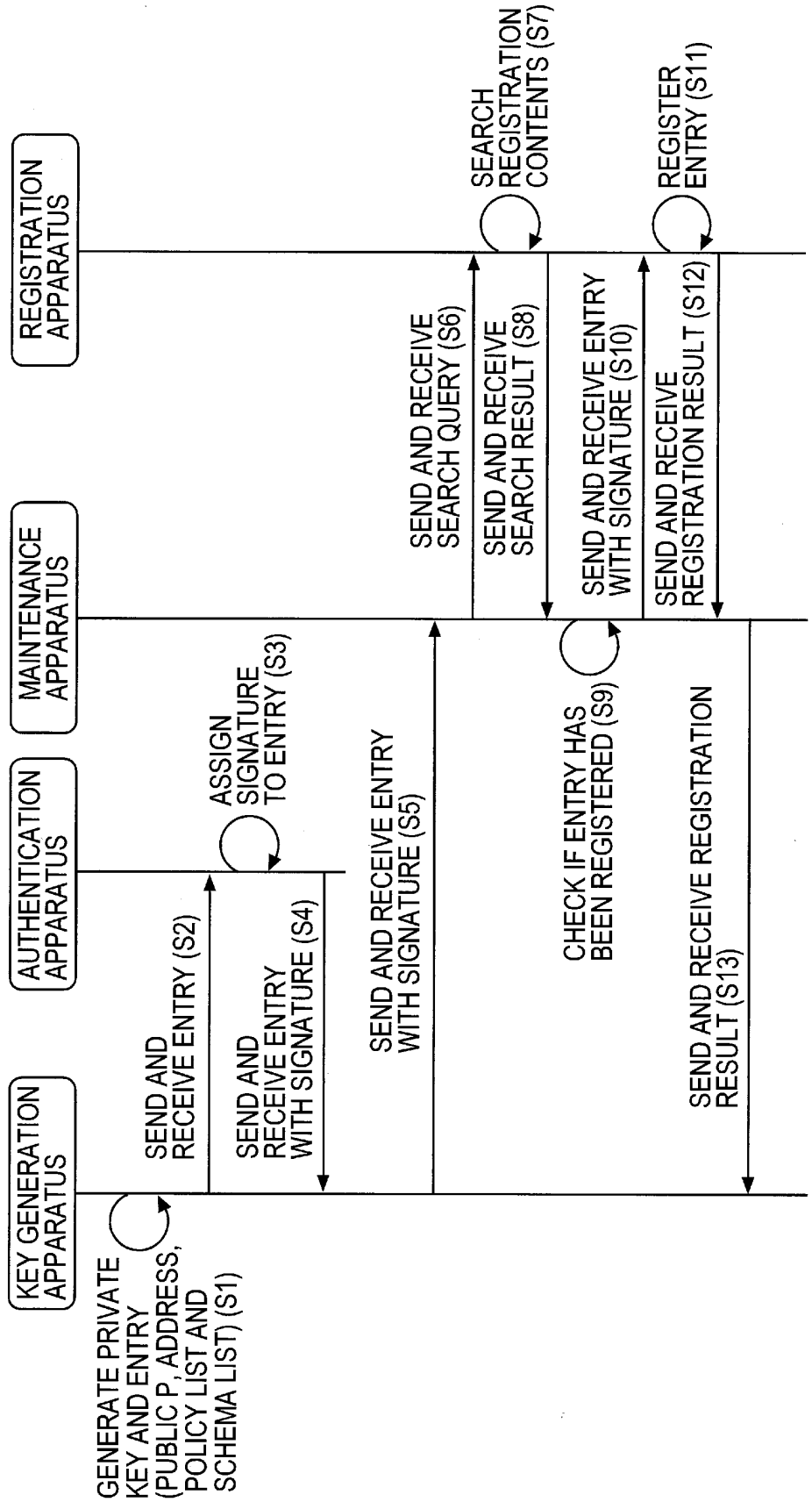

KEY GENERATION APPARATUS
AUTHENTICATION APPARATUS
MAINTENANCE APPARATUS
REGISTRATION APPARATUS
GENERATE PRIVATE KEY AND ENTRY (PUBLIC P, ADDRESS, POLICY LIST AND SCHEMA LIST) (S1)
SEND AND RECEIVE ENTRY (S2)
ASSIGN SIGNATURE TO ENTRY (S3)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S4)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S5)
SEND AND RECEIVE SEARCH QUERY (S6)
SEARCH REGISTRATION CONTENTS (S7)
SEND AND RECEIVE SEARCH RESULT (S8)
CHECK IF ENTRY HAS BEEN REGISTERED (S9)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S10)
REGISTER ENTRY (S11)
SEND AND RECEIVE REGISTRATION RESULT (S12)
SEND AND RECEIVE REGISTRATION RESULT (S13)

FIG.30

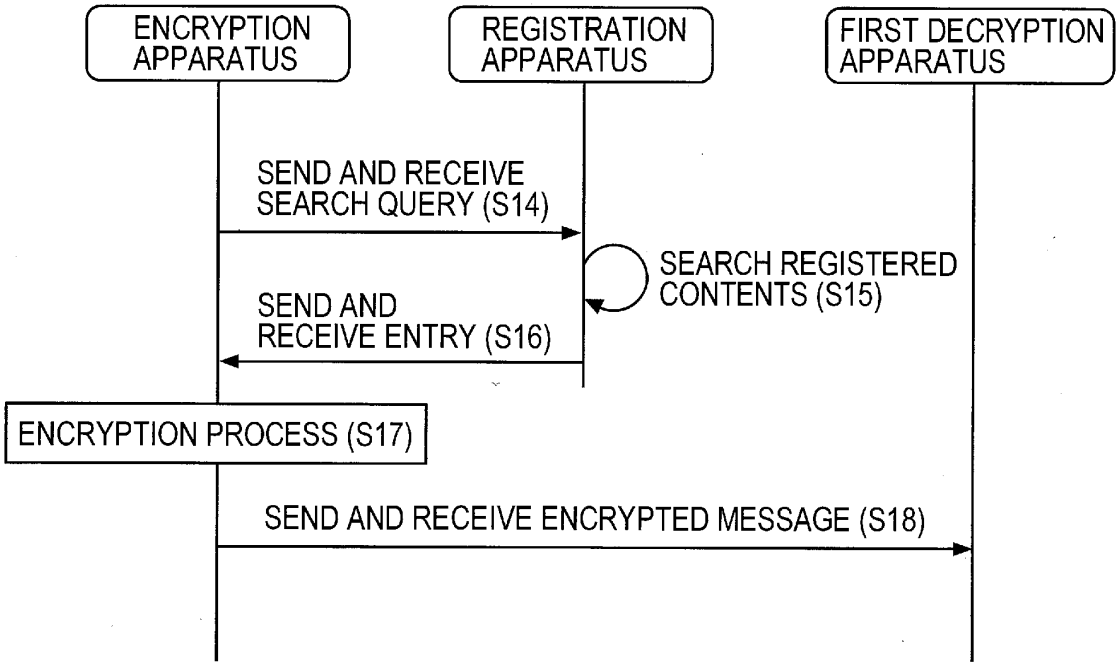

ENCRYPTION APPARATUS
REGISTRATION APPARATUS
FIRST DECRYPTION APPARATUS
SEND AND RECEIVE SEARCH QUERY (S14)
SEARCH REGISTERED CONTENTS (S15)
SEND AND RECEIVE ENTRY (S16)
ENCRYPTION PROCESS (S17)
SEND AND RECEIVE ENCRYPTED MESSAGE (S18)

FIG.31

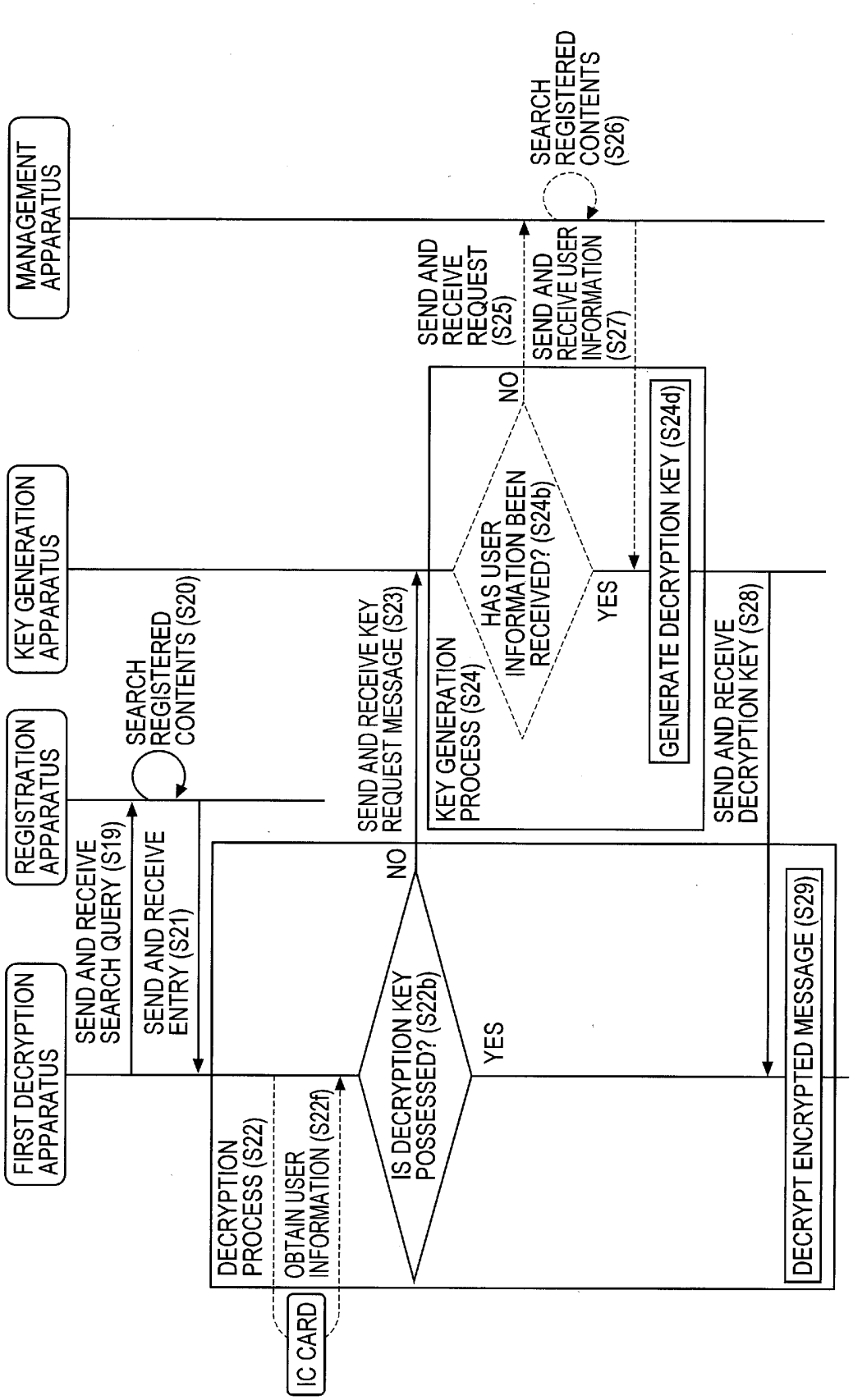

FIRST DECRYPTION APPARATUS
REGISTRATION APPARATUS
KEY GENERATION APPARATUS
MANAGEMENT APPARATUS
SEND AND RECEIVE SEARCH QUERY (S19)
SEARCH REGISTERED CONTENTS (S20)
SEND AND RECEIVE ENTRY (S21)
DECRYPTION PROCESS (S22)
OBTAIN USER INFORMATION (S22f)
IC CARD
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
SEND AND RECEIVE KEY REQUEST MESSAGE (S23)
KEY GENERATION PROCESS (S24)
HAS USER INFORMATION BEEN RECEIVED? (S24b)
NO
YES
SEND AND RECEIVE REQUEST (S25)
SEARCH REGISTERED CONTENTS (S26)
SEND AND RECEIVE USER INFORMATION (S27)
GENERATE DECRYPTION KEY (S24d)
SEND AND RECEIVE DECRYPTION KEY (S28)
DECRYPT ENCRYPTED MESSAGE (S29)

FIG.32

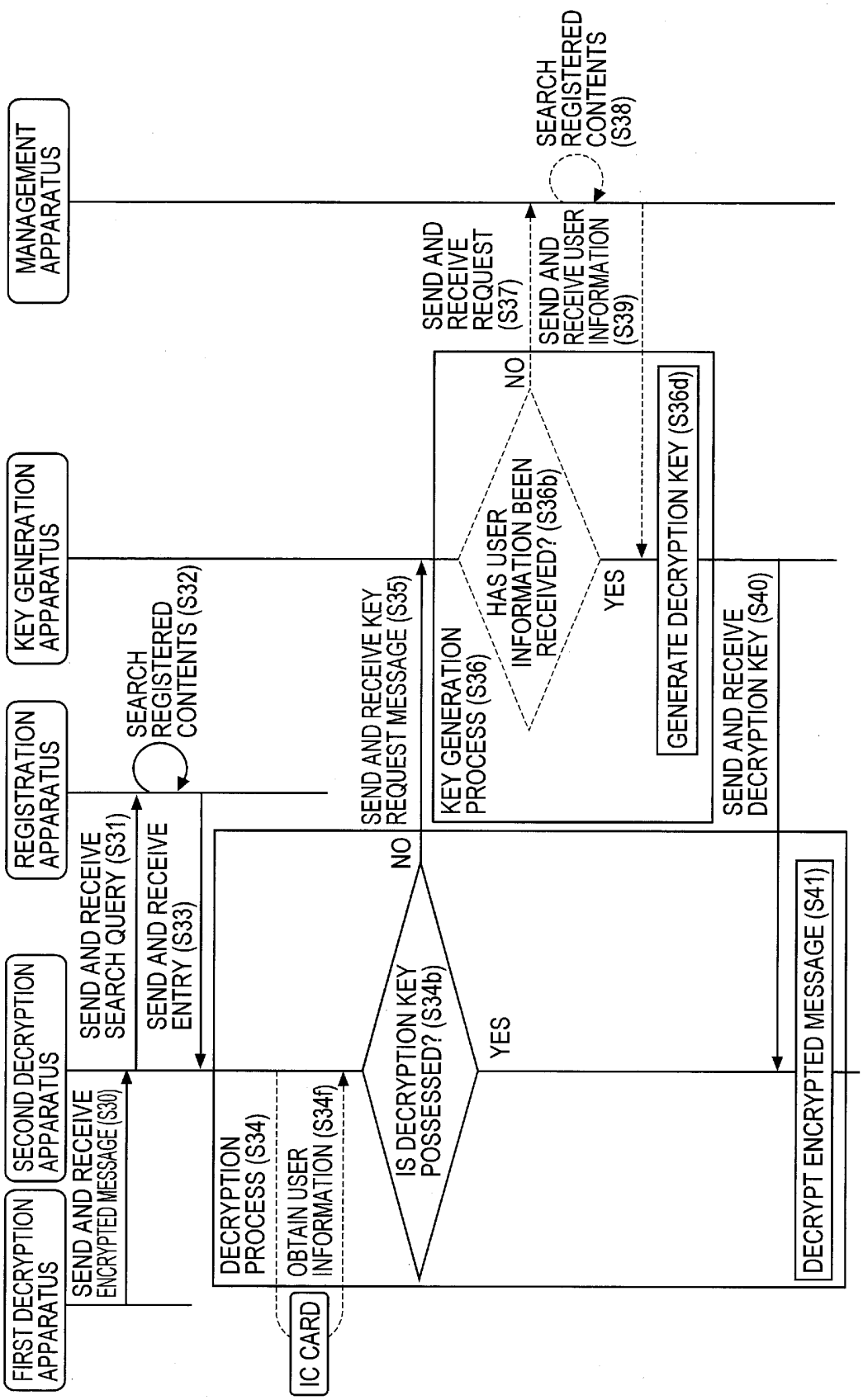

FIRST DECRYPTION APPARATUS
SECOND DECRYPTION APPARATUS
REGISTRATION APPARATUS
KEY GENERATION APPARATUS
MANAGEMENT APPARATUS
SEND AND RECEIVE ENCRYPTED MESSAGE (S30)
SEND AND RECEIVE SEARCH QUERY (S31)
SEARCH REGISTERED CONTENTS (S32)
SEND AND RECEIVE ENTRY (S33)
DECRYPTION PROCESS (S34)
OBTAIN USER INFORMATION (S34f)
IC CARD
IS DECRYPTION KEY POSSESSED? (S34b)
NO
YES
SEND AND RECEIVE KEY REQUEST MESSAGE (S35)
KEY GENERATION PROCESS (S36)
HAS USER INFORMATION BEEN RECEIVED? (S36b)
NO
YES
SEND AND RECEIVE REQUEST (S37)
SEARCH REGISTERED CONTENTS (S38)
SEND AND RECEIVE USER INFORMATION (S39)
GENERATE DECRYPTION KEY (S36d)
SEND AND RECEIVE DECRYPTION KEY (S40)
DECRYPT ENCRYPTED MESSAGE (S41)

FIG.33

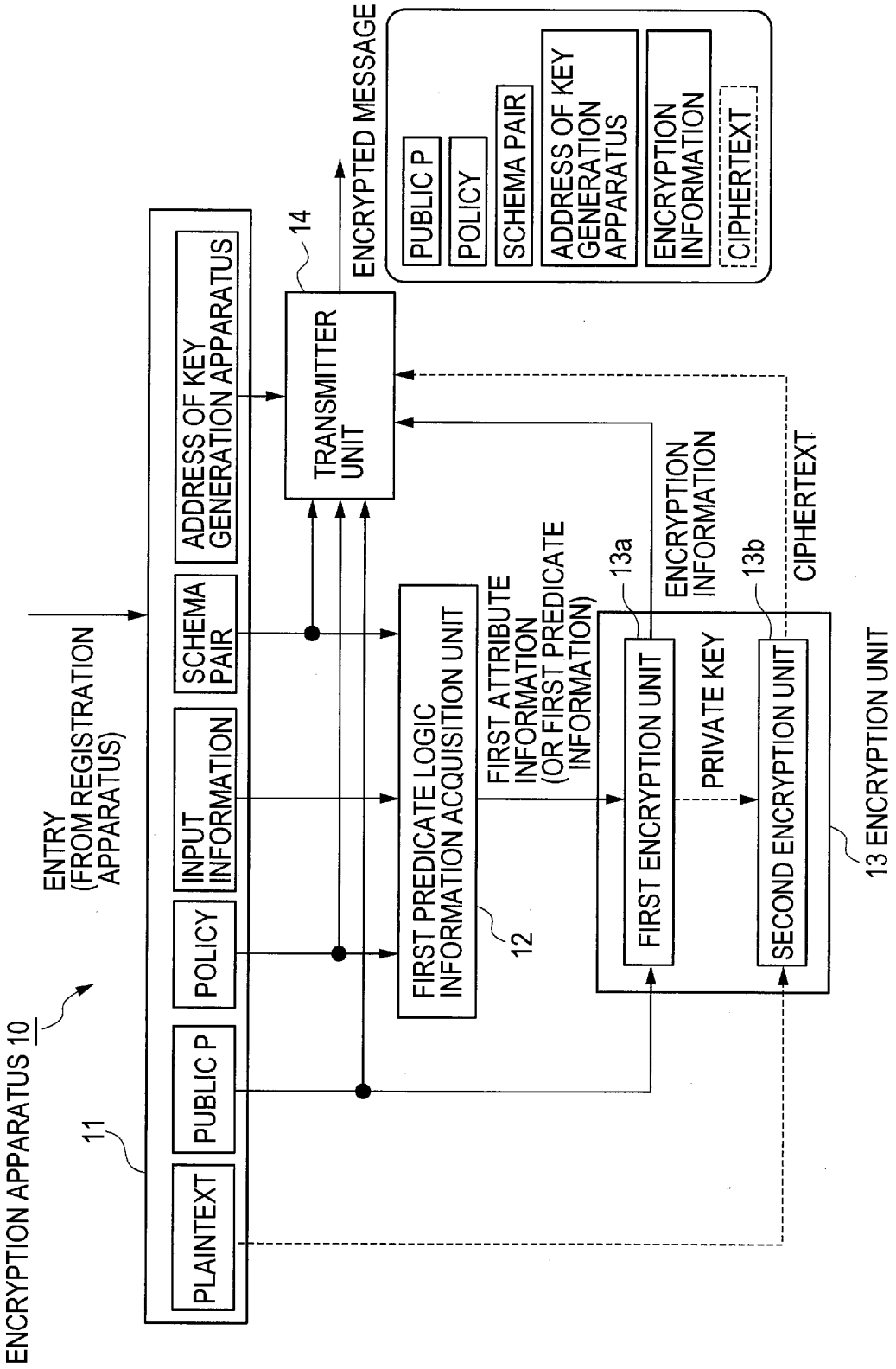

ENCRYPTION APPARATUS 10
11
ENTRY (FROM REGISTRATION APPARATUS)
PLAINTEXT
PUBLIC P
POLICY
INPUT INFORMATION
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
FIRST PREDICATE LOGIC INFORMATION ACQUISITION UNIT
12
FIRST ATTRIBUTE INFORMATION (OR FIRST PREDICATE INFORMATION)
TRANSMITTER UNIT
14
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
CIPHERTEXT
13a
FIRST ENCRYPTION UNIT
PRIVATE KEY
13b
SECOND ENCRYPTION UNIT
ENCRYPTION INFORMATION
CIPHERTEXT
13 ENCRYPTION UNIT

FIG.34

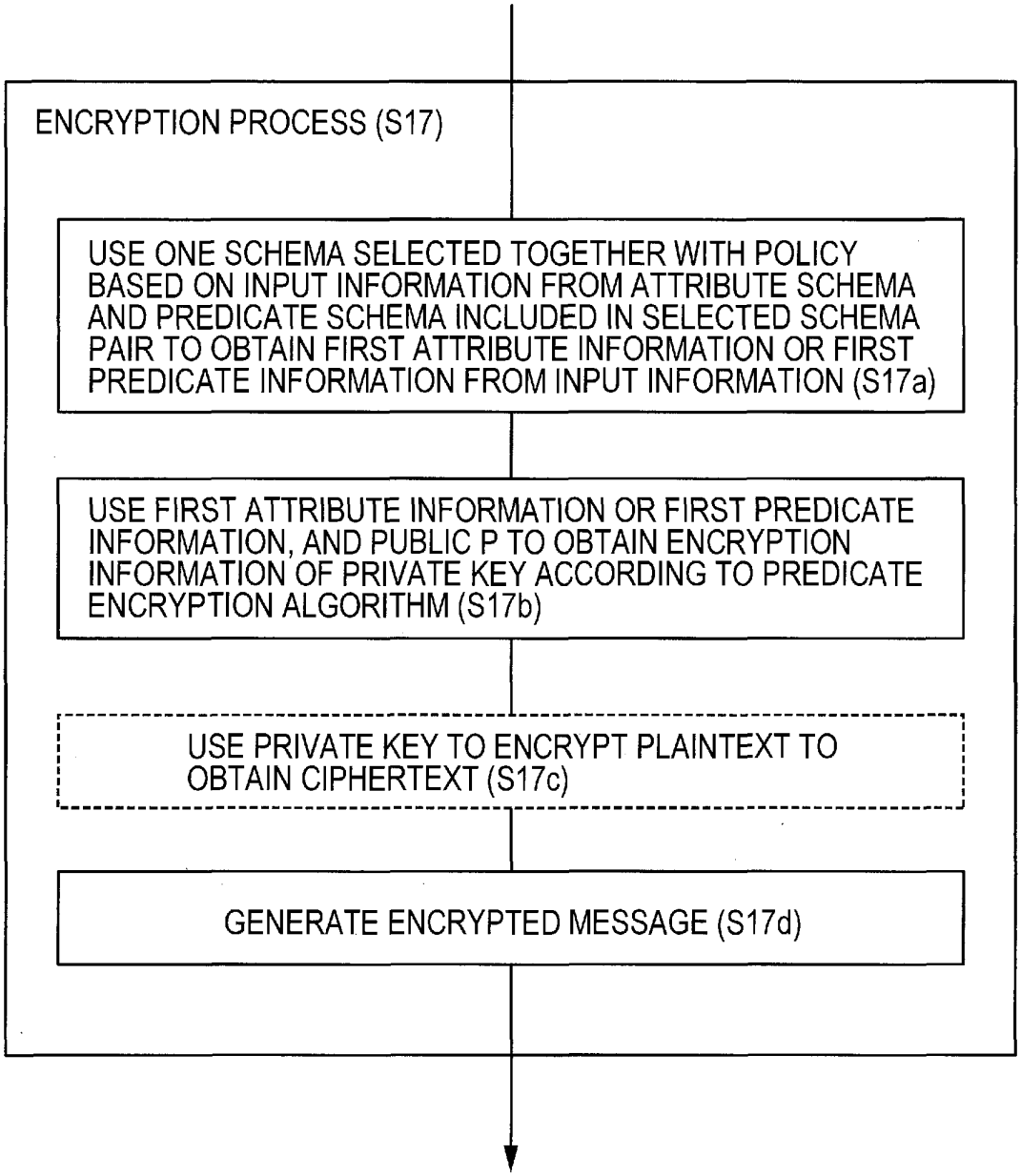

ENCRYPTION PROCESS (S17)
USE ONE SCHEMA SELECTED TOGETHER WITH POLICY BASED ON INPUT INFORMATION FROM ATTRIBUTE SCHEMA AND PREDICATE SCHEMA INCLUDED IN SELECTED SCHEMA PAIR TO OBTAIN FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION FROM INPUT INFORMATION (S17a)
USE FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION, AND PUBLIC P TO OBTAIN ENCRYPTION INFORMATION OF PRIVATE KEY ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S17b)
USE PRIVATE KEY TO ENCRYPT PLAINTEXT TO OBTAIN CIPHERTEXT (S17c)
GENERATE ENCRYPTED MESSAGE (S17d)

FIG.35

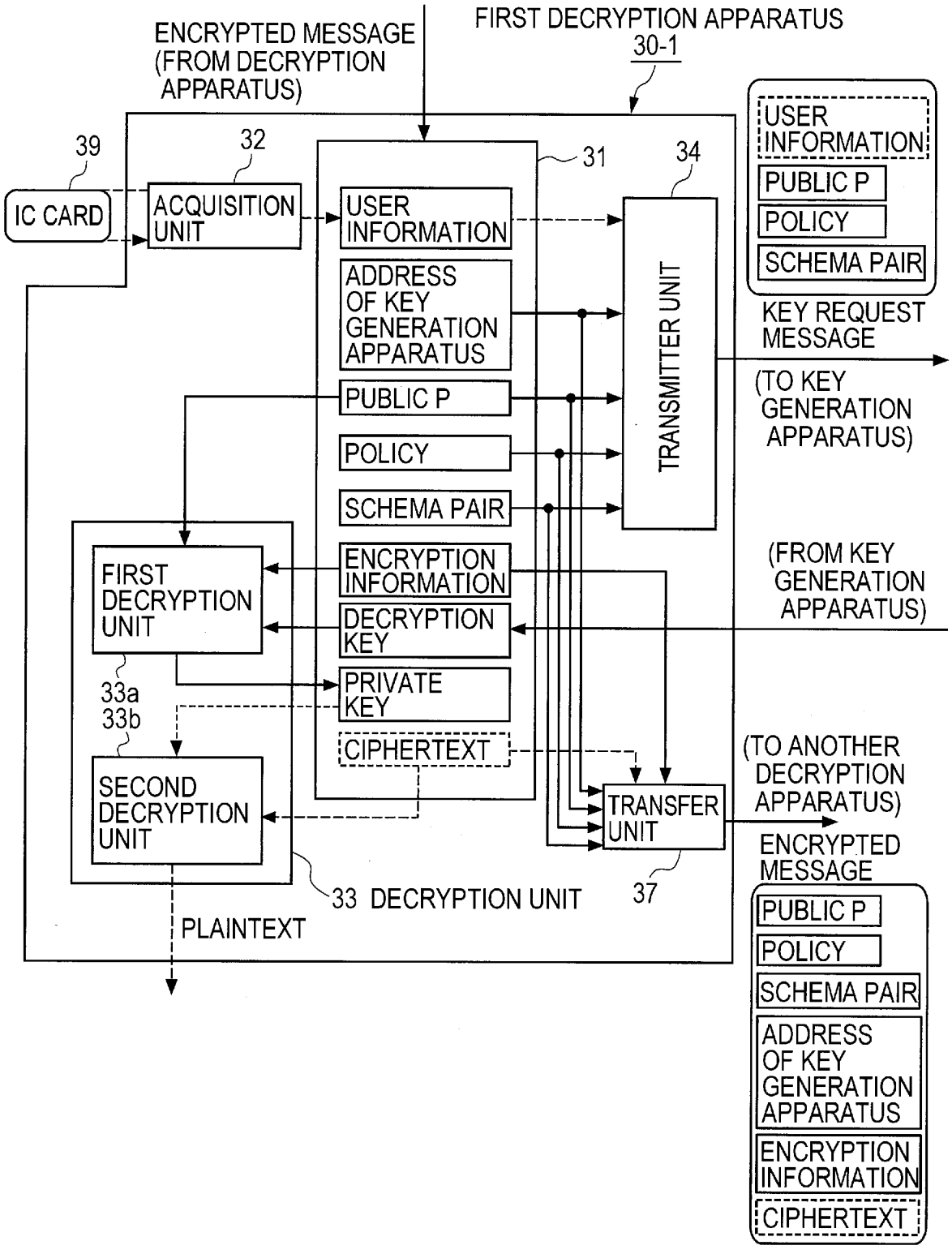

ENCRYPTED MESSAGE (FROM DECRYPTION APPARATUS)
FIRST DECRYPTION APPARATUS
30-1
39
32
31
34
IC CARD
ACQUISITION UNIT
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
(FROM KEY GENERATION APPARATUS)
FIRST DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
PRIVATE KEY
CIPHERTEXT
33a
33b
SECOND DECRYPTION UNIT
TRANSFER UNIT
(TO ANOTHER DECRYPTION APPARATUS)
ENCRYPTED MESSAGE
33 DECRYPTION UNIT
37
PLAINTEXT
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
CIPHERTEXT

FIG.36

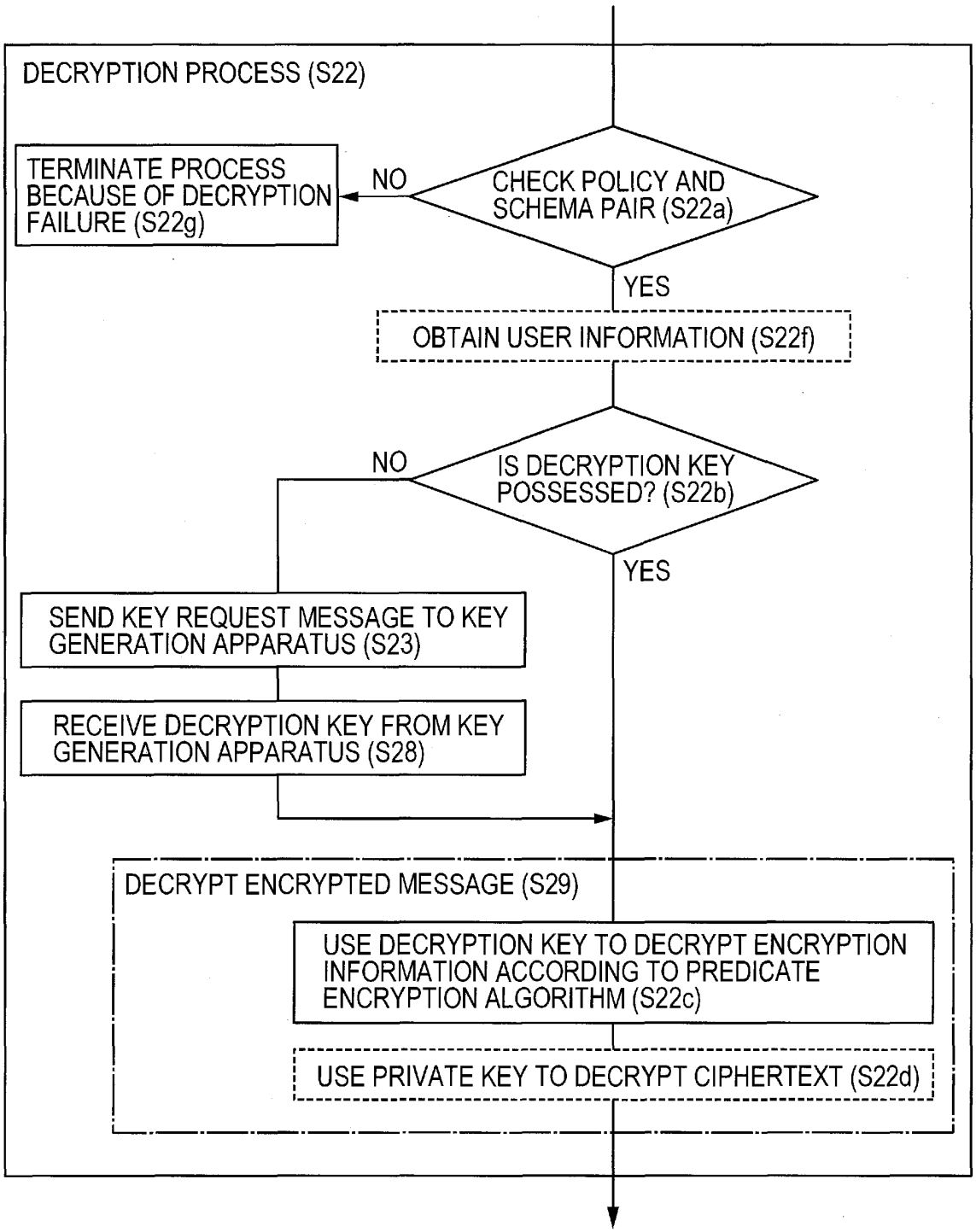

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c)
USE PRIVATE KEY TO DECRYPT CIPHERTEXT (S22d)

FIG.37

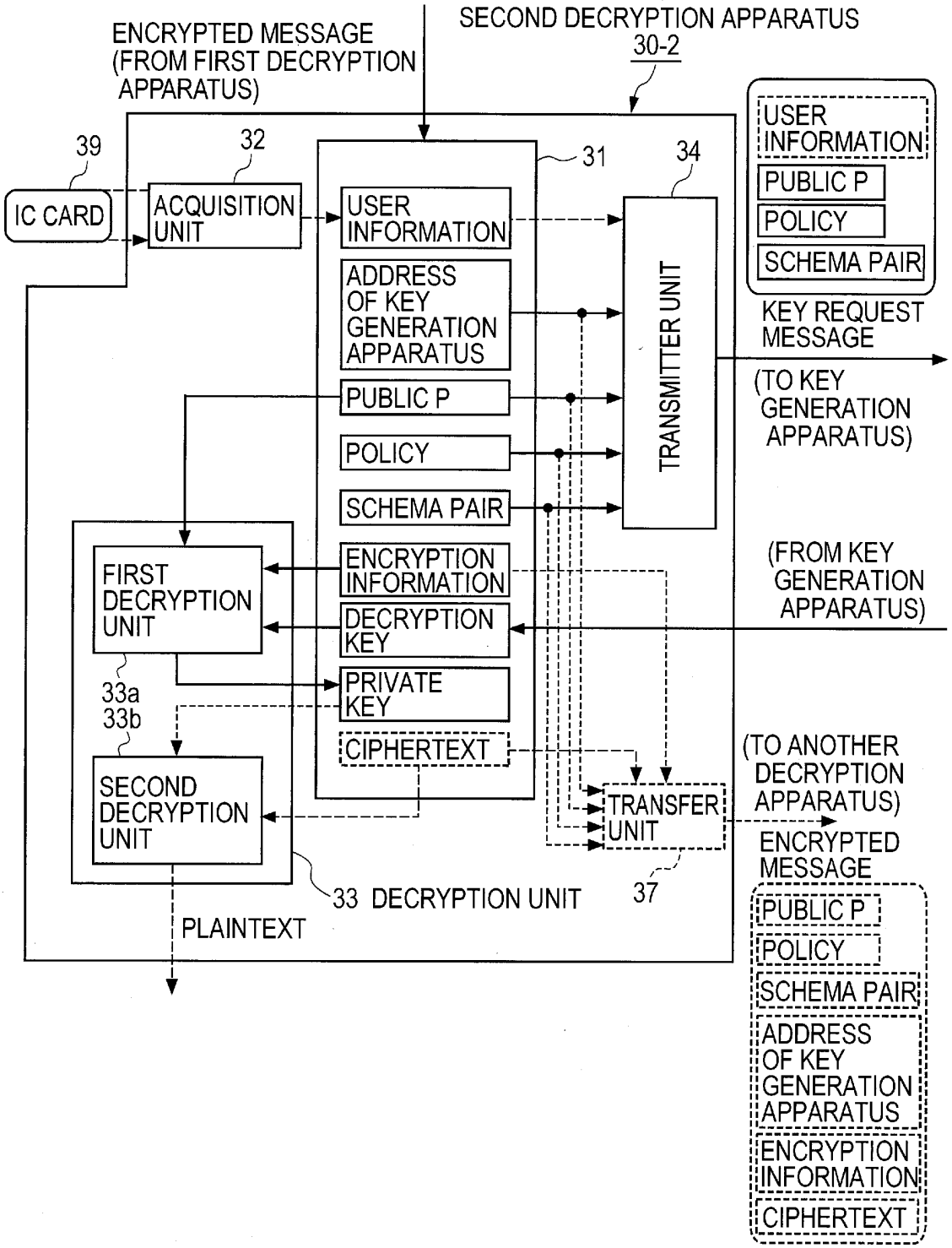

ENCRYPTED MESSAGE (FROM FIRST DECRYPTION APPARATUS)
SECOND DECRYPTION APPARATUS
30-2
39
32
31
34
IC CARD
ACQUISITION UNIT
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
(FROM KEY GENERATION APPARATUS)
FIRST DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
PRIVATE KEY
CIPHERTEXT
33a
33b
SECOND DECRYPTION UNIT
TRANSFER UNIT
(TO ANOTHER DECRYPTION APPARATUS)
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
CIPHERTEXT
33 DECRYPTION UNIT
37
PLAINTEXT

FIG.38

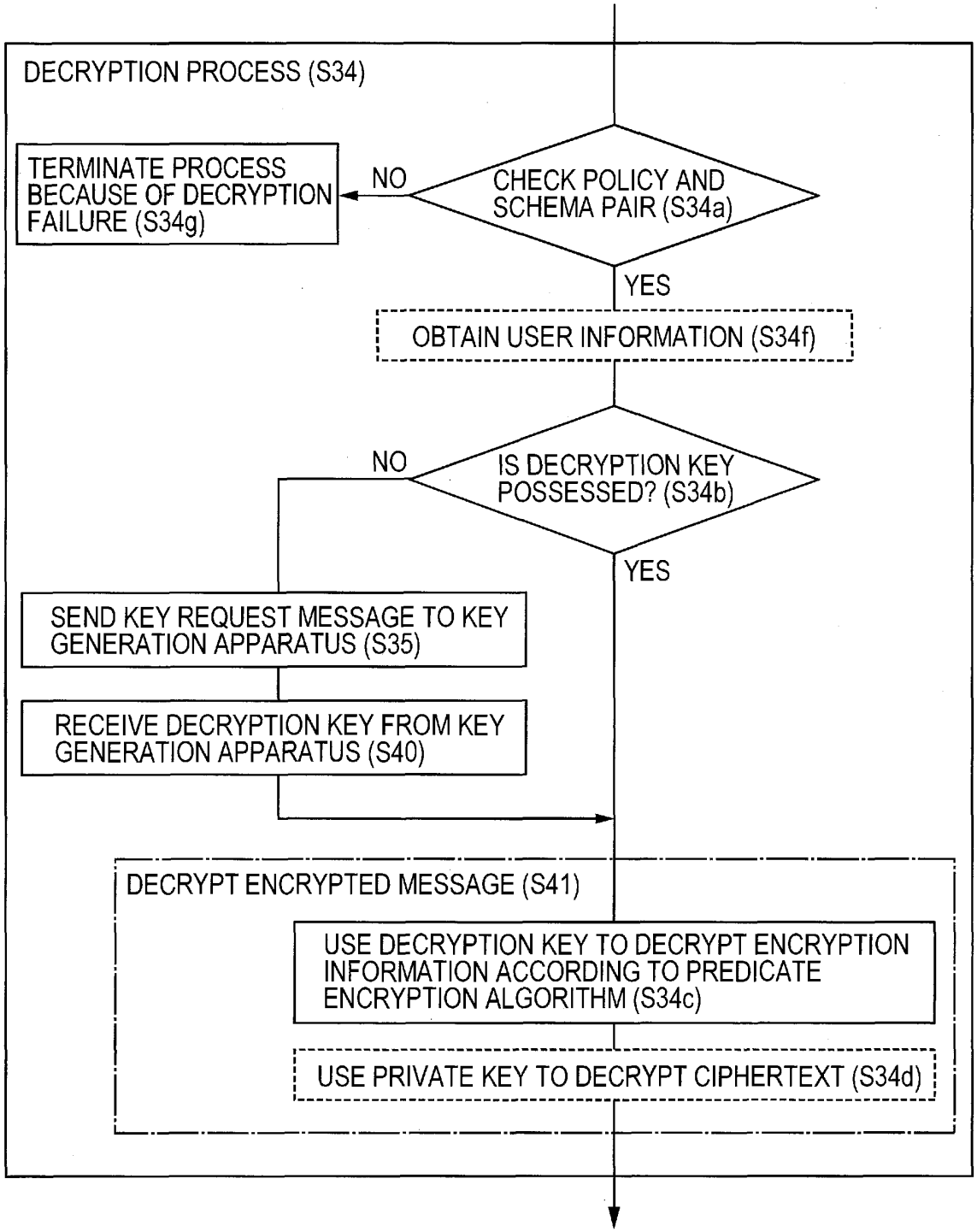

DECRYPTION PROCESS (S34)
CHECK POLICY AND SCHEMA PAIR (S34a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S34g)
YES
OBTAIN USER INFORMATION (S34f)
IS DECRYPTION KEY POSSESSED? (S34b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S35)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S40)
DECRYPT ENCRYPTED MESSAGE (S41)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S34c)
USE PRIVATE KEY TO DECRYPT CIPHERTEXT (S34d)

FIG.39

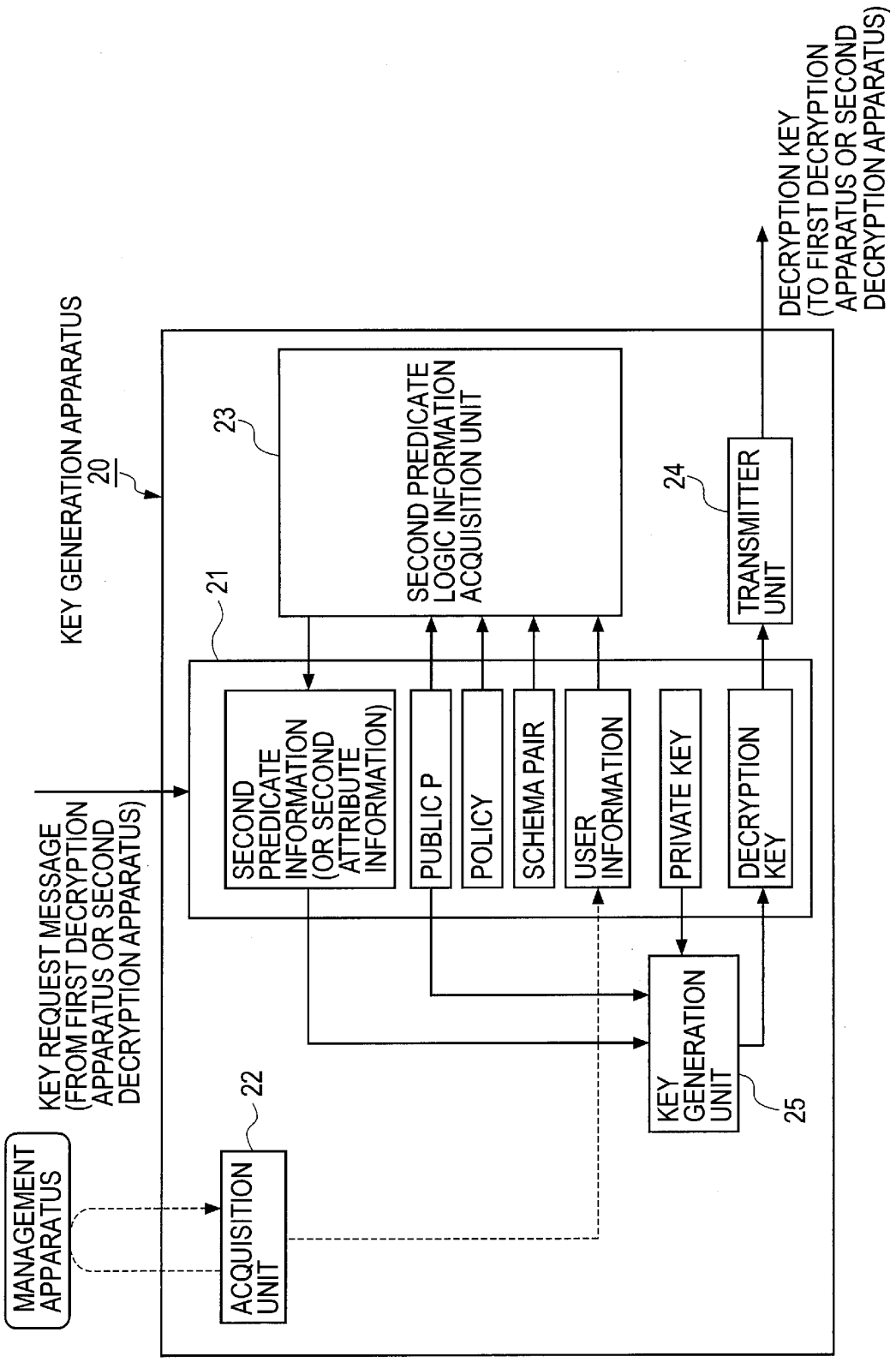

MANAGEMENT APPARATUS
KEY REQUEST MESSAGE (FROM FIRST DECRYPTION APPARATUS OR SECOND DECRYPTION APPARATUS)
KEY GENERATION APPARATUS
20
ACQUISITION UNIT
22
21
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
PRIVATE KEY
DECRYPTION KEY
23
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
24
TRANSMITTER UNIT
KEY GENERATION UNIT
25
DECRYPTION KEY (TO FIRST DECRYPTION APPARATUS OR SECOND DECRYPTION APPARATUS)

FIG.40

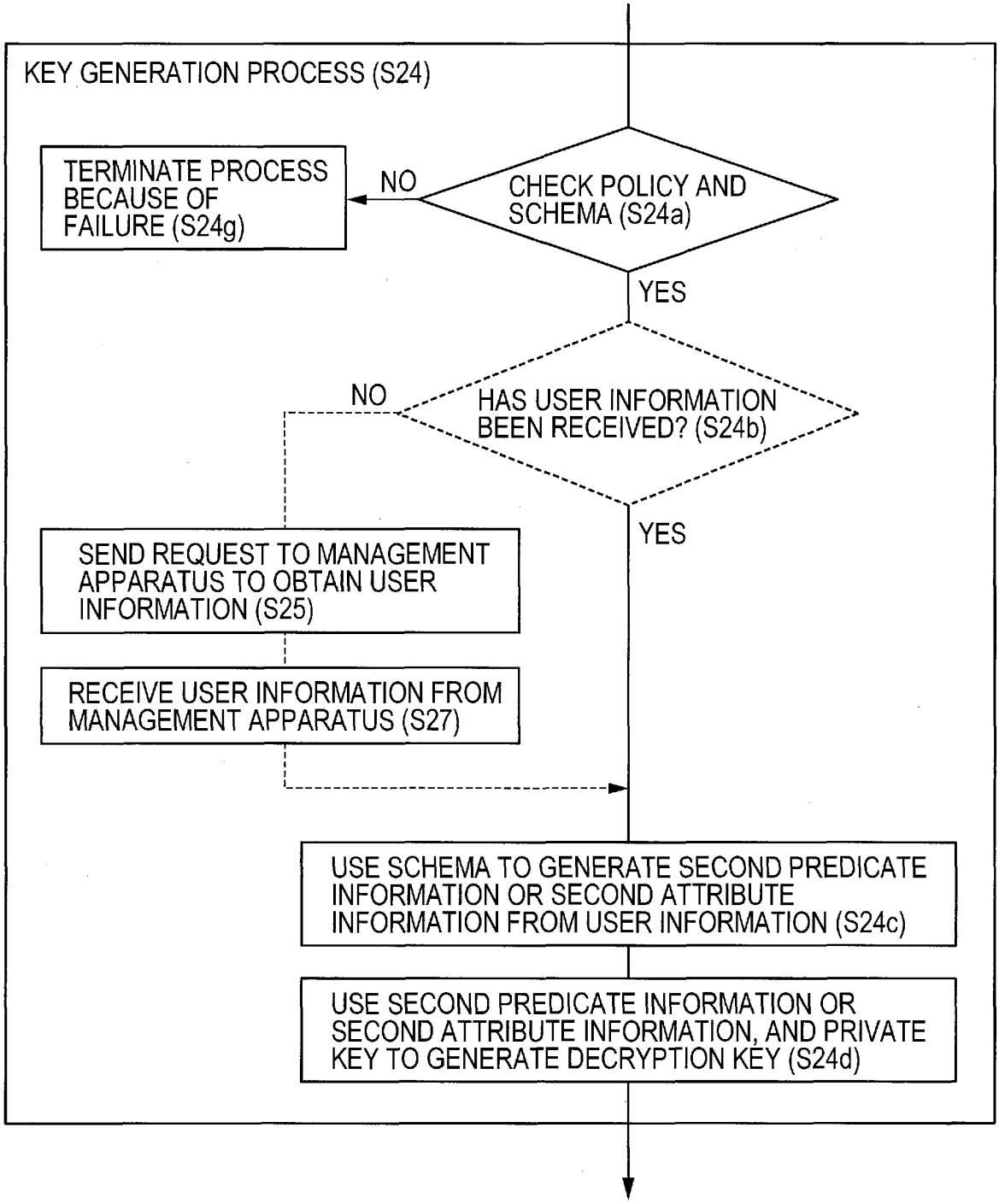

KEY GENERATION PROCESS (S24)
CHECK POLICY AND SCHEMA (S24a)
NO
TERMINATE PROCESS BECAUSE OF FAILURE (S24g)
YES
HAS USER INFORMATION BEEN RECEIVED? (S24b)
NO
YES
SEND REQUEST TO MANAGEMENT APPARATUS TO OBTAIN USER INFORMATION (S25)
RECEIVE USER INFORMATION FROM MANAGEMENT APPARATUS (S27)
USE SCHEMA TO GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION FROM USER INFORMATION (S24c)
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S24d)

FIG.41

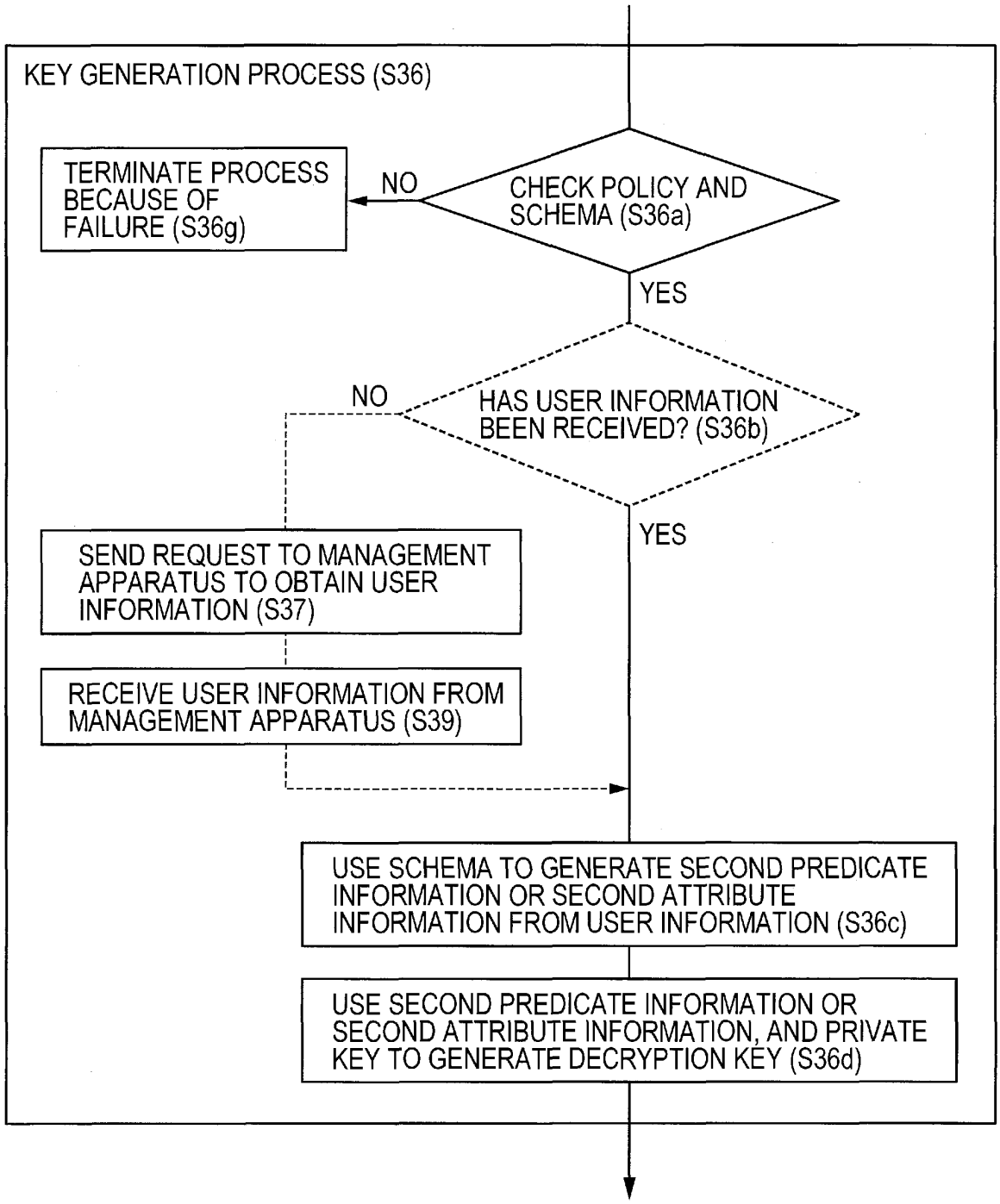

KEY GENERATION PROCESS (S36)
CHECK POLICY AND SCHEMA (S36a)
NO
TERMINATE PROCESS BECAUSE OF FAILURE (S36g)
YES
HAS USER INFORMATION BEEN RECEIVED? (S36b)
NO
YES
SEND REQUEST TO MANAGEMENT APPARATUS TO OBTAIN USER INFORMATION (S37)
RECEIVE USER INFORMATION FROM MANAGEMENT APPARATUS (S39)
USE SCHEMA TO GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION FROM USER INFORMATION (S36c)
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S36d)

FIG.42

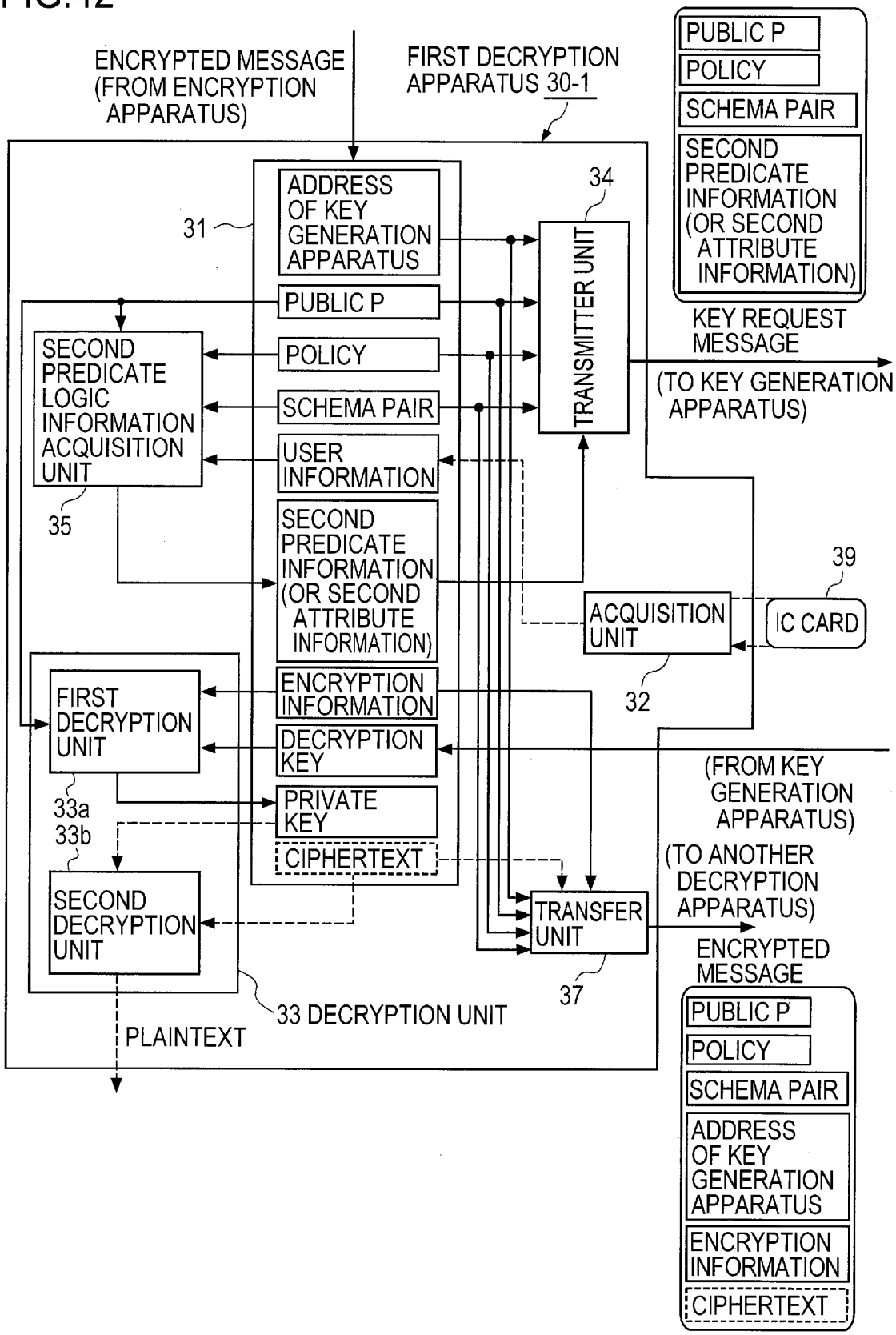

ENCRYPTED MESSAGE (FROM ENCRYPTION APPARATUS)
FIRST DECRYPTION APPARATUS 30-1
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
31
ADDRESS OF KEY GENERATION APPARATUS
34
TRANSMITTER UNIT
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
39
ACQUISITION UNIT
IC CARD
32
FIRST DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
(FROM KEY GENERATION APPARATUS)
33a
33b
PRIVATE KEY
CIPHERTEXT
(TO ANOTHER DECRYPTION APPARATUS)
SECOND DECRYPTION UNIT
TRANSFER UNIT
ENCRYPTED MESSAGE
37
33 DECRYPTION UNIT
PLAINTEXT
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
CIPHERTEXT

FIG.43

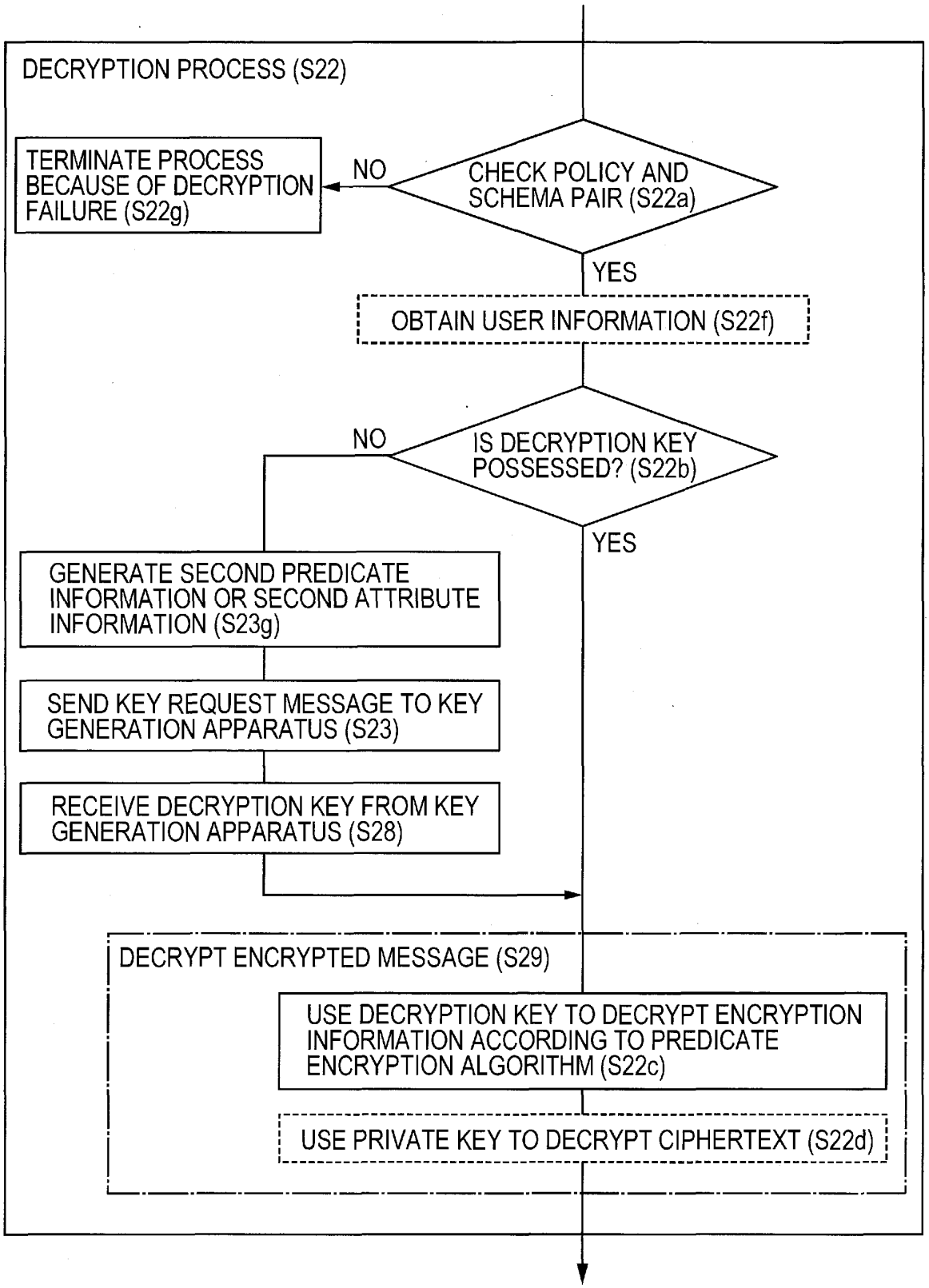

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S23g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c)
USE PRIVATE KEY TO DECRYPT CIPHERTEXT (S22d)

FIG.44

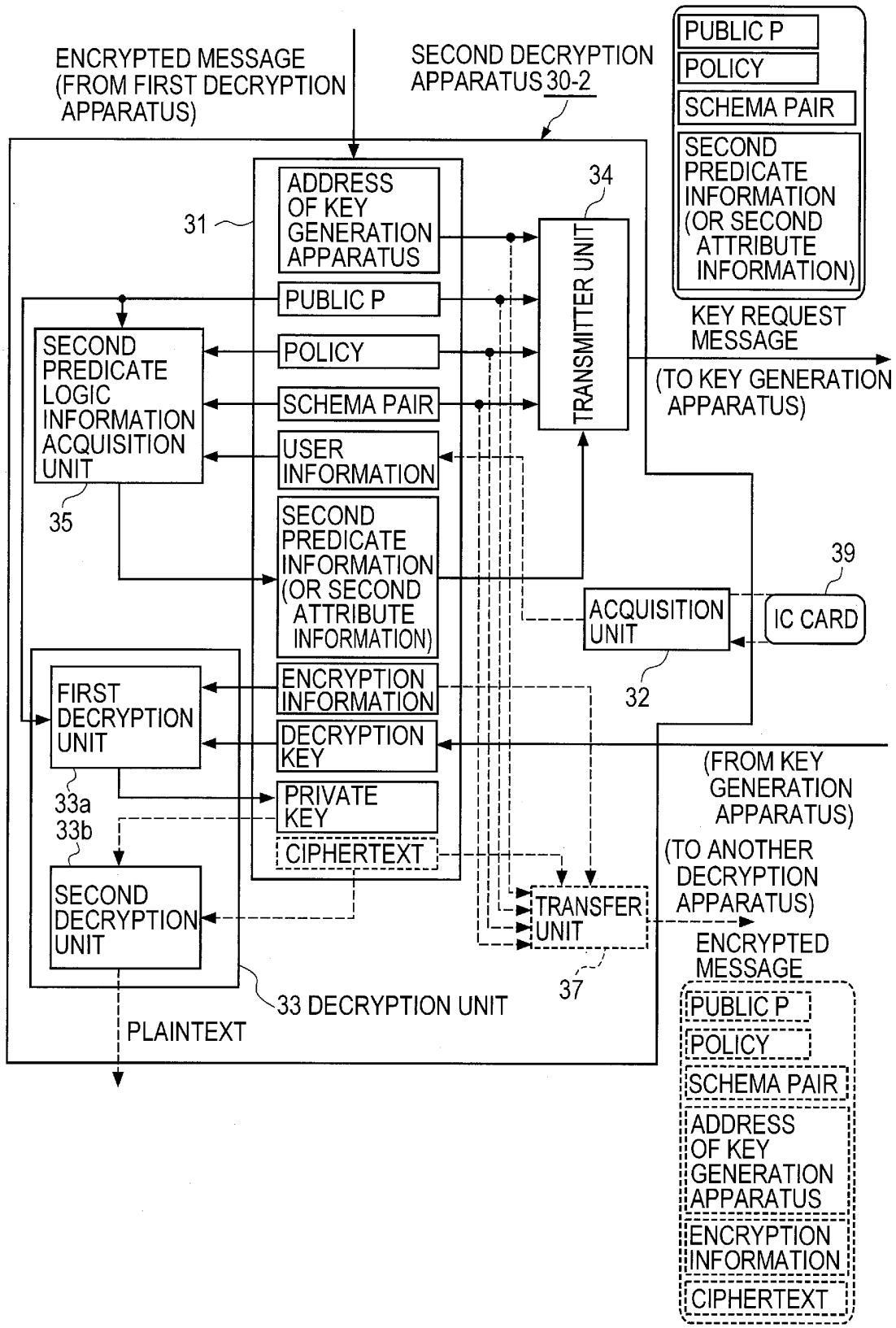

ENCRYPTED MESSAGE (FROM FIRST DECRYPTION APPARATUS)
SECOND DECRYPTION APPARATUS 30-2
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
31
ADDRESS OF KEY GENERATION APPARATUS
34
TRANSMITTER UNIT
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
39
ACQUISITION UNIT
IC CARD
32
ENCRYPTION INFORMATION
DECRYPTION KEY
FIRST DECRYPTION UNIT
33a
33b
PRIVATE KEY
CIPHERTEXT
(FROM KEY GENERATION APPARATUS)
(TO ANOTHER DECRYPTION APPARATUS)
SECOND DECRYPTION UNIT
TRANSFER UNIT
37
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
CIPHERTEXT
33 DECRYPTION UNIT
PLAINTEXT

FIG.45

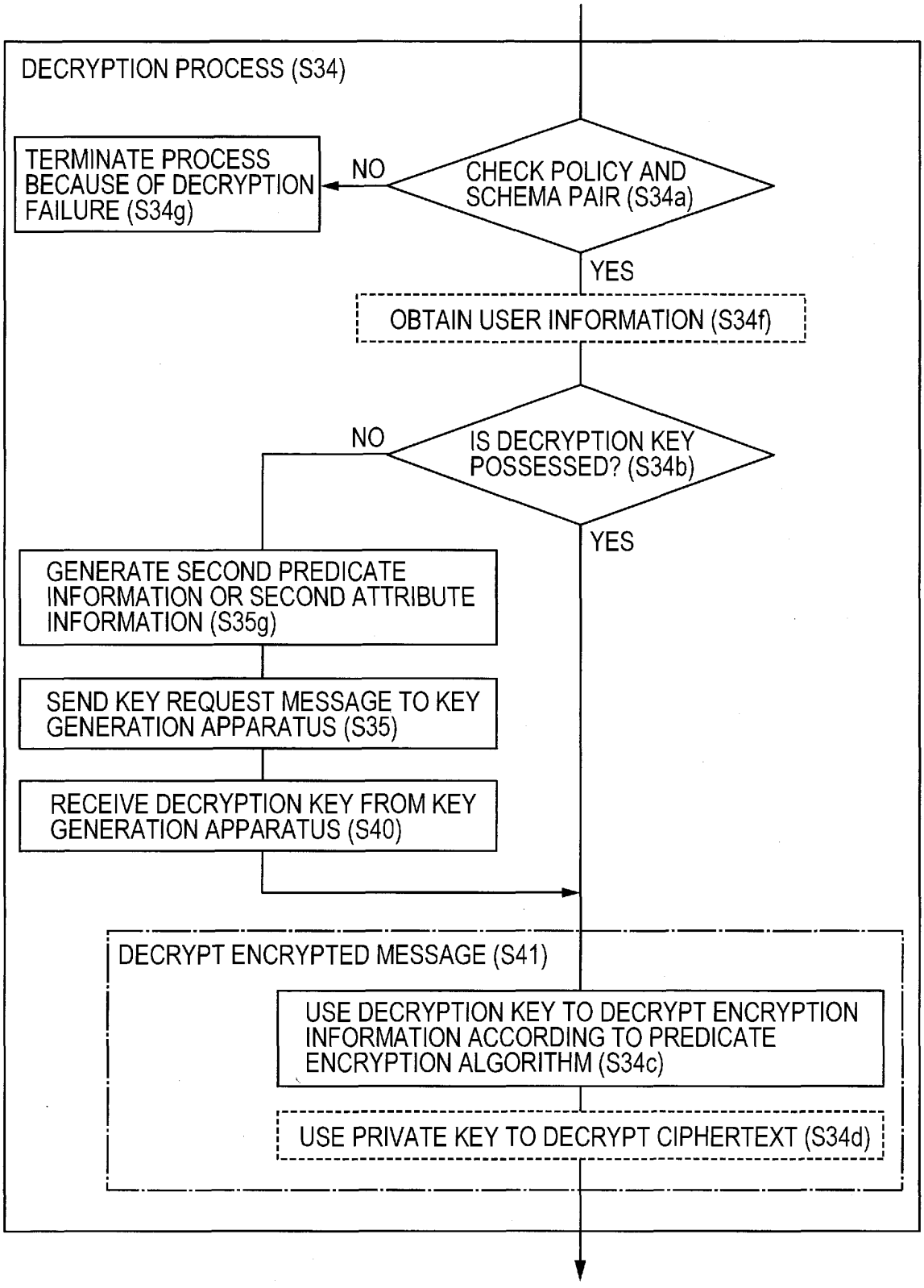

DECRYPTION PROCESS (S34)
CHECK POLICY AND SCHEMA PAIR (S34a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S34g)
YES
OBTAIN USER INFORMATION (S34f)
IS DECRYPTION KEY POSSESSED? (S34b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S35g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S35)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S40)
DECRYPT ENCRYPTED MESSAGE (S41)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S34c)
USE PRIVATE KEY TO DECRYPT CIPHERTEXT (S34d)

FIG.46

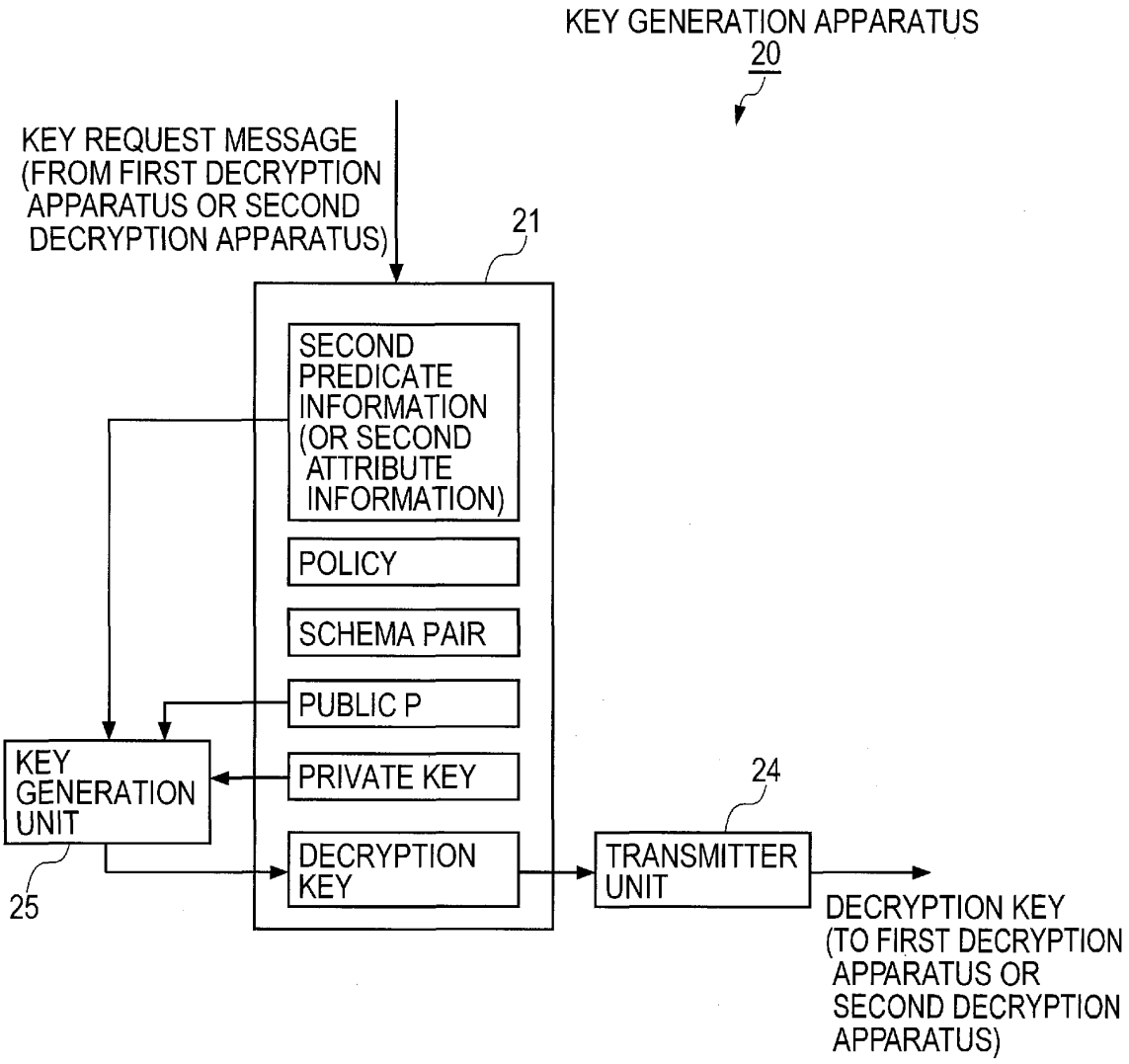

KEY GENERATION APPARATUS
20
KEY REQUEST MESSAGE (FROM FIRST DECRYPTION APPARATUS OR SECOND DECRYPTION APPARATUS)
21
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
POLICY
SCHEMA PAIR
PUBLIC P
PRIVATE KEY
DECRYPTION KEY
KEY GENERATION UNIT
25
24
TRANSMITTER UNIT
DECRYPTION KEY (TO FIRST DECRYPTION APPARATUS OR SECOND DECRYPTION APPARATUS)

FIG.47

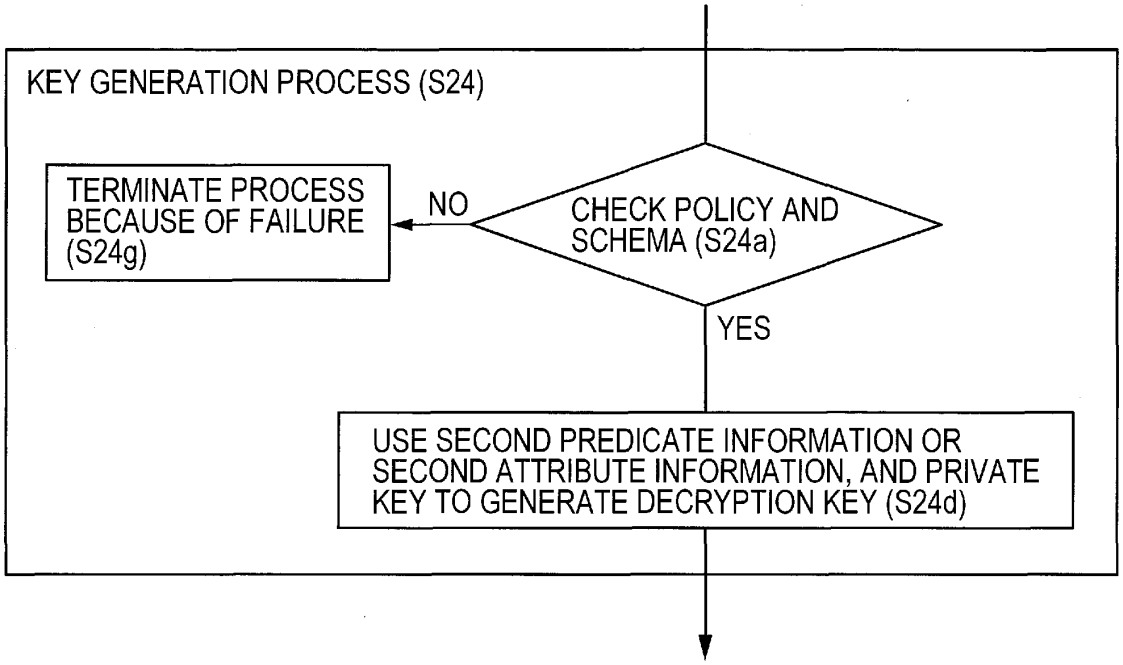

KEY GENERATION PROCESS (S24)
TERMINATE PROCESS BECAUSE OF FAILURE (S24g)
NO
CHECK POLICY AND SCHEMA (S24a)
YES
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S24d)

FIG.48

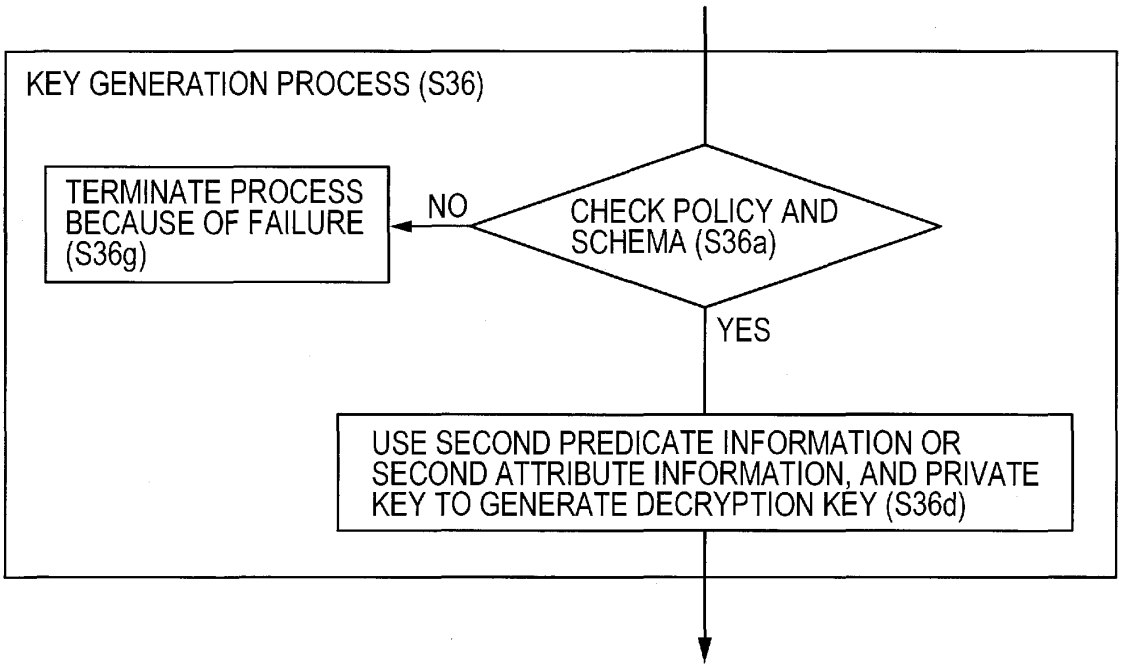

KEY GENERATION PROCESS (S36)
TERMINATE PROCESS BECAUSE OF FAILURE (S36g)
NO
CHECK POLICY AND SCHEMA (S36a)
YES
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S36d)

FIG.49

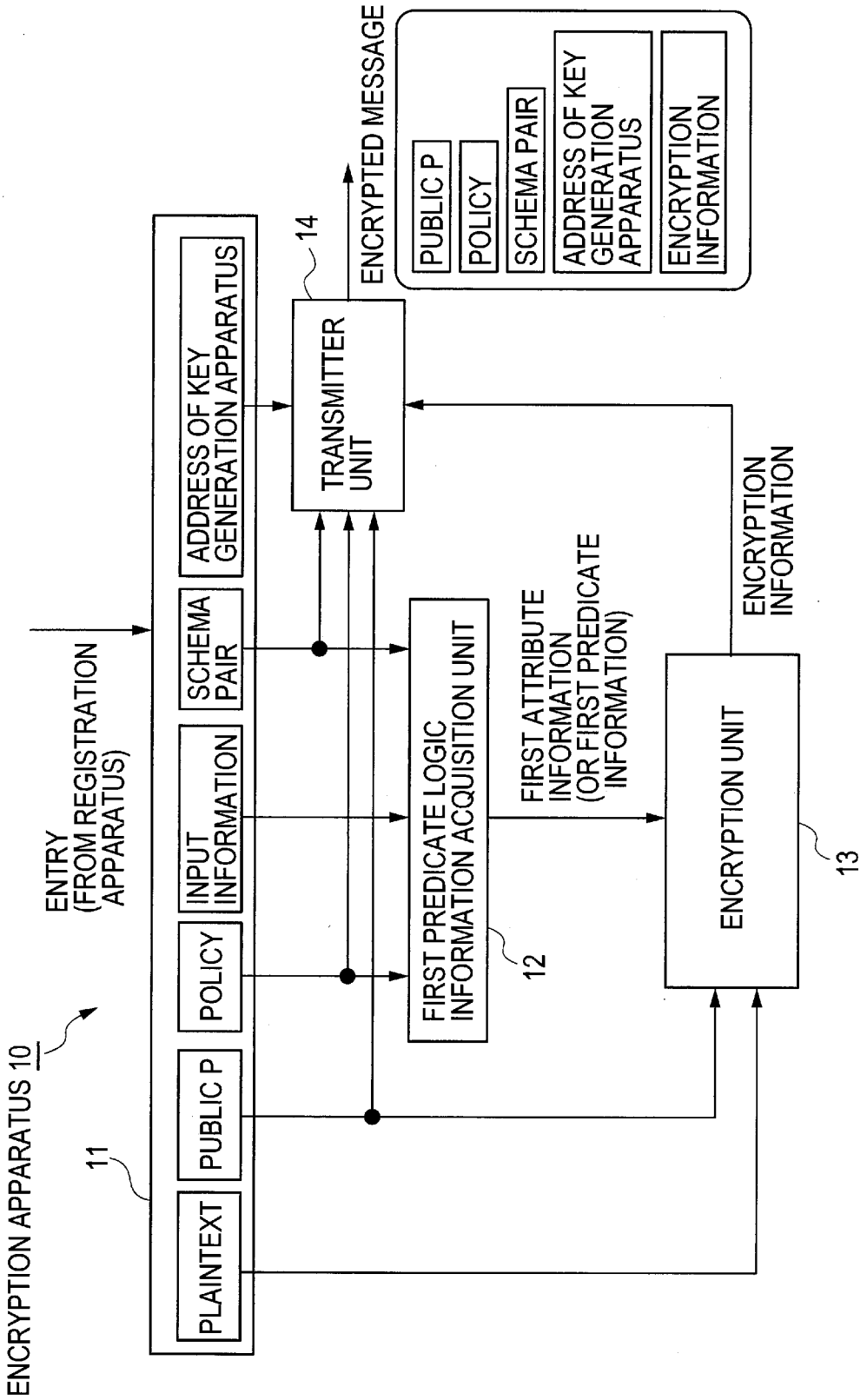

ENCRYPTION APPARATUS 10
ENTRY (FROM REGISTRATION APPARATUS)
11
PLAINTEXT
PUBLIC P
POLICY
INPUT INFORMATION
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
FIRST PREDICATE LOGIC INFORMATION ACQUISITION UNIT
12
FIRST ATTRIBUTE INFORMATION (OR FIRST PREDICATE INFORMATION)
ENCRYPTION UNIT
13
ENCRYPTION INFORMATION
TRANSMITTER UNIT
14
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION

FIG.50

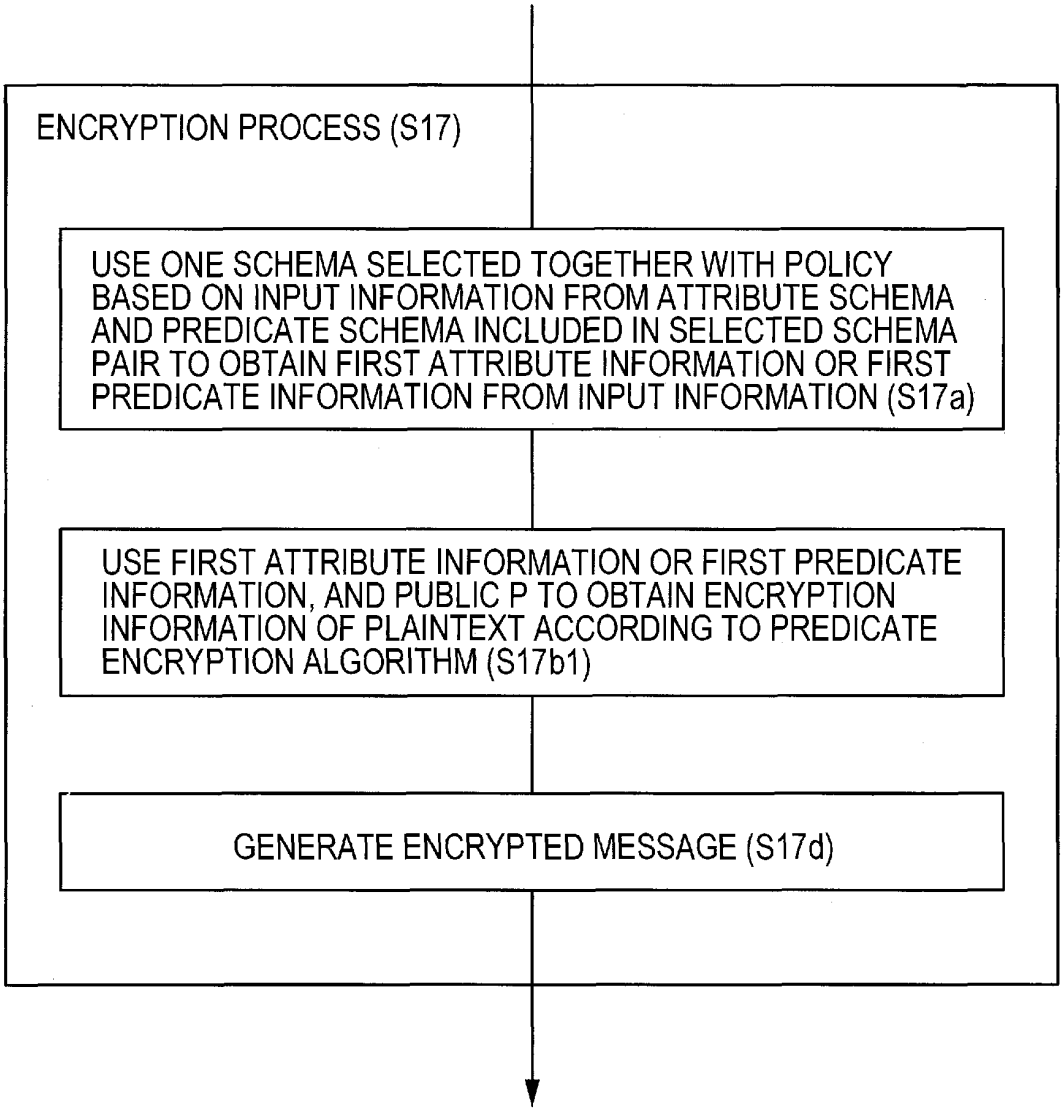

ENCRYPTION PROCESS (S17)
USE ONE SCHEMA SELECTED TOGETHER WITH POLICY BASED ON INPUT INFORMATION FROM ATTRIBUTE SCHEMA AND PREDICATE SCHEMA INCLUDED IN SELECTED SCHEMA PAIR TO OBTAIN FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION FROM INPUT INFORMATION (S17a)
USE FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION, AND PUBLIC P TO OBTAIN ENCRYPTION INFORMATION OF PLAINTEXT ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S17b1)
GENERATE ENCRYPTED MESSAGE (S17d)

FIG.51

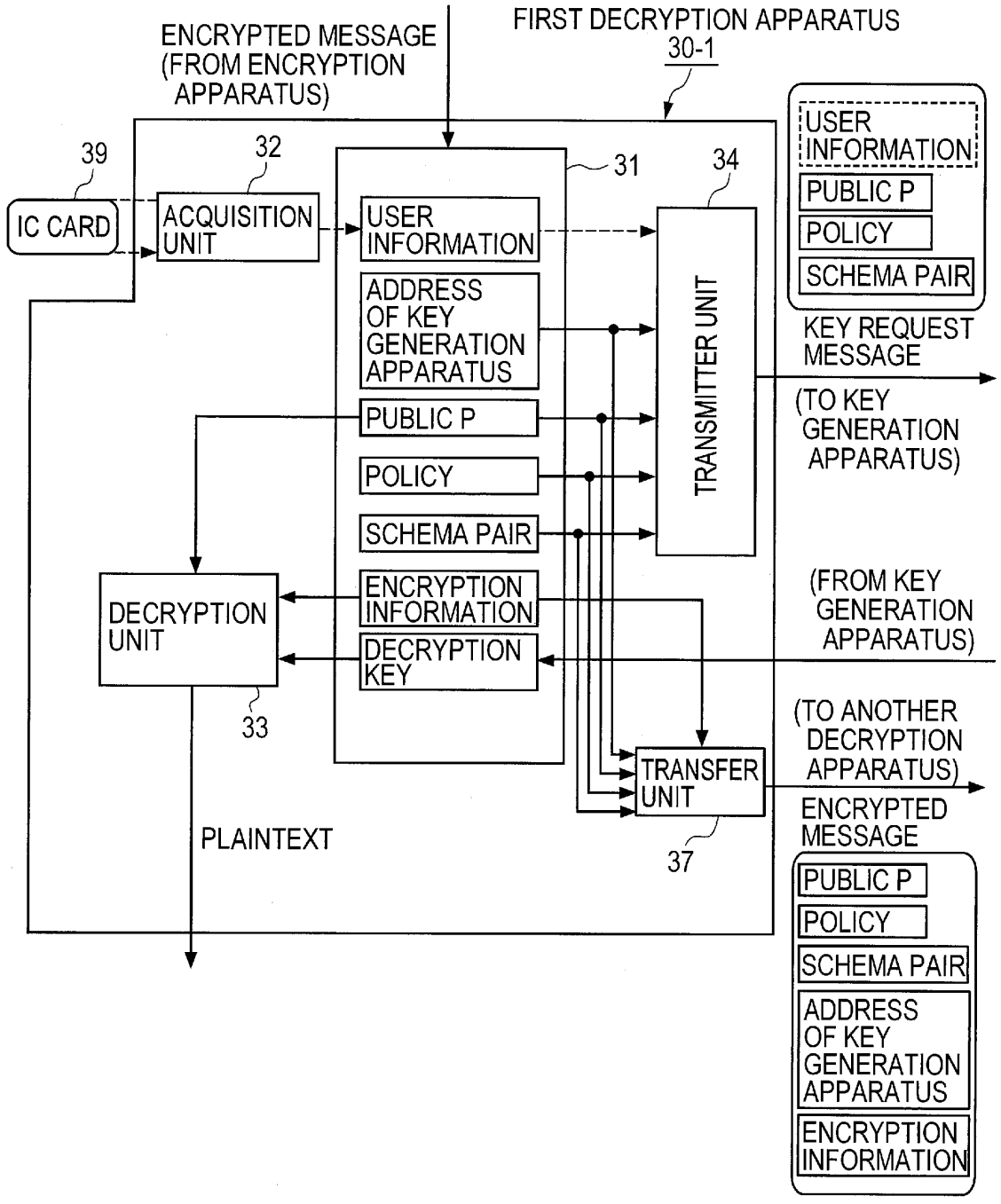

ENCRYPTED MESSAGE (FROM ENCRYPTION APPARATUS)
FIRST DECRYPTION APPARATUS
30-1
39
32
31
34
IC CARD
ACQUISITION UNIT
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
(FROM KEY GENERATION APPARATUS)
33
(TO ANOTHER DECRYPTION APPARATUS)
TRANSFER UNIT
ENCRYPTED MESSAGE
PLAINTEXT
37
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION

FIG.52

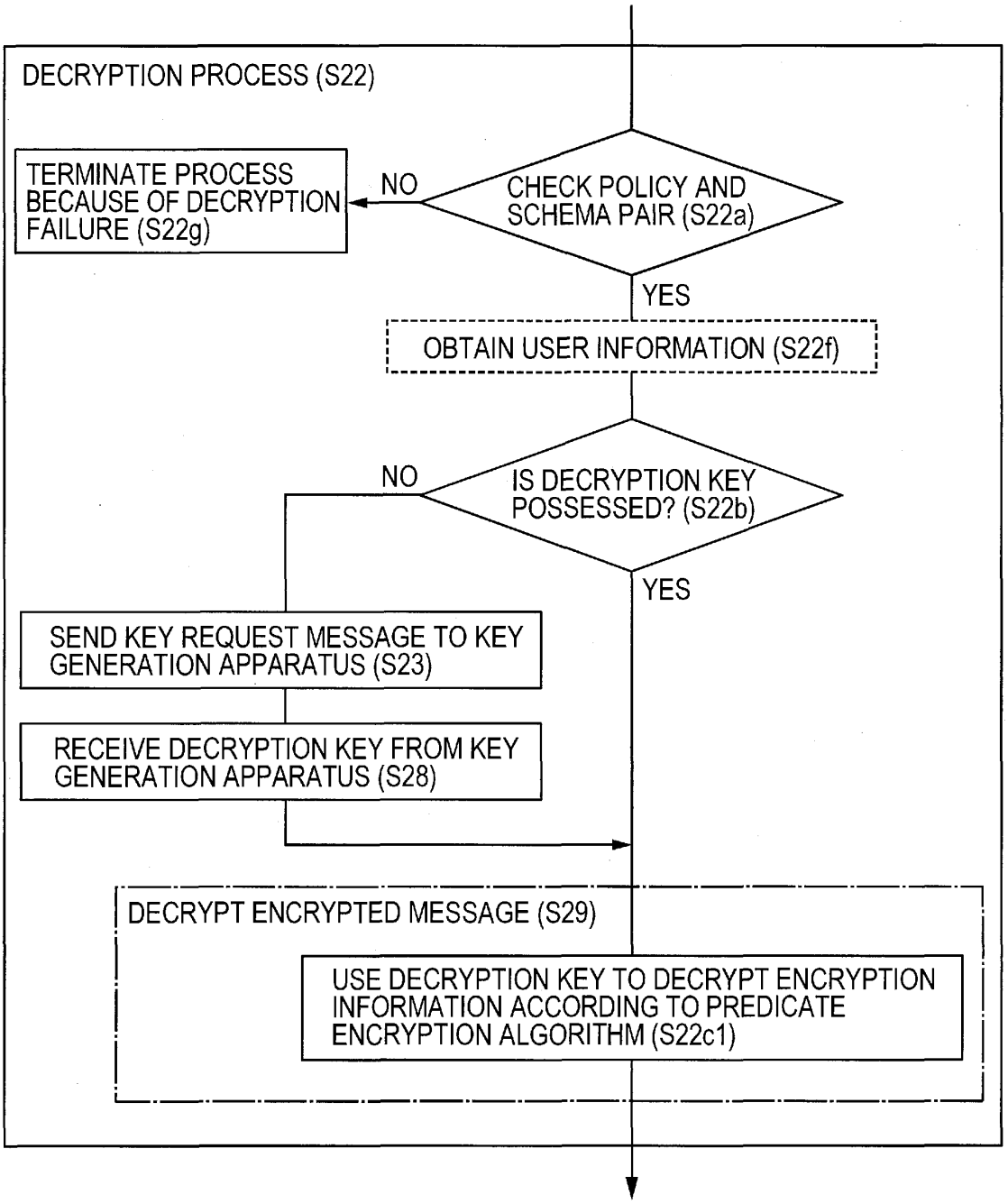

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c1)

FIG.53

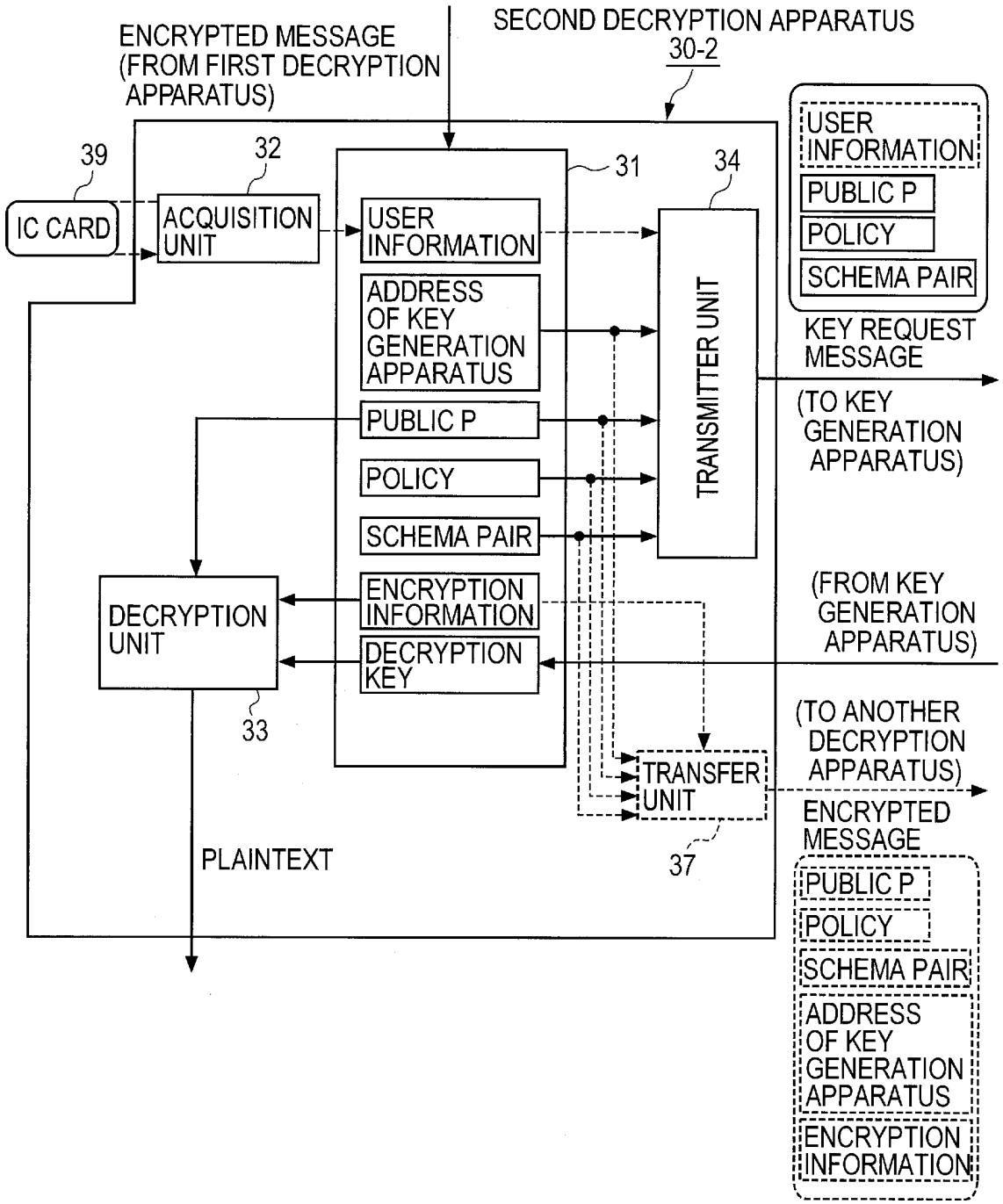

ENCRYPTED MESSAGE
(FROM FIRST DECRYPTION APPARATUS)
SECOND DECRYPTION APPARATUS
30-2
39
32
31
34
IC CARD
ACQUISITION UNIT
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
(FROM KEY GENERATION APPARATUS)
33
(TO ANOTHER DECRYPTION APPARATUS)
TRANSFER UNIT
ENCRYPTED MESSAGE
37
PLAINTEXT
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION

FIG.54

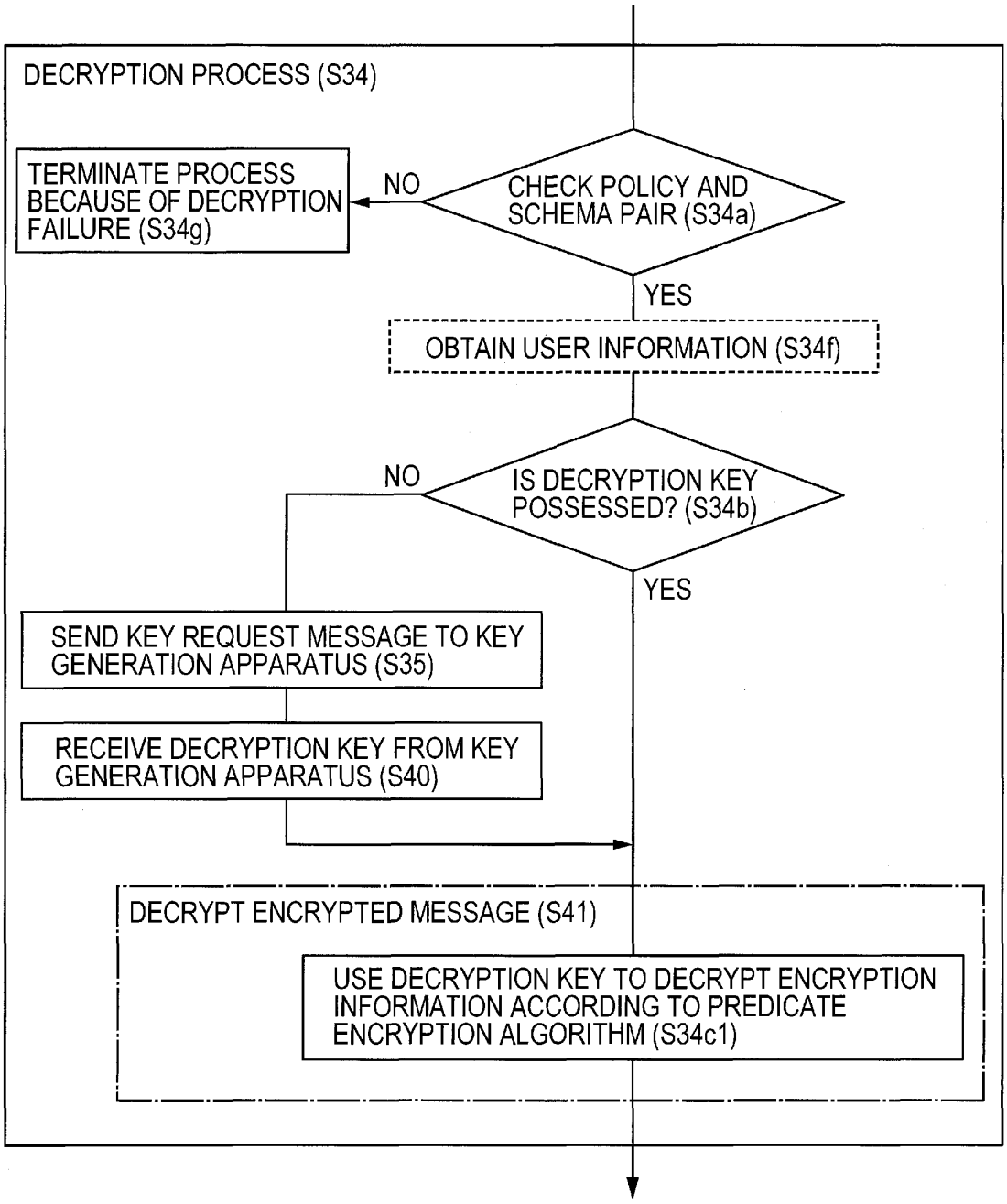

DECRYPTION PROCESS (S34)
CHECK POLICY AND SCHEMA PAIR (S34a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S34g)
YES
OBTAIN USER INFORMATION (S34f)
IS DECRYPTION KEY POSSESSED? (S34b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S35)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S40)
DECRYPT ENCRYPTED MESSAGE (S41)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S34c1)

FIG.55

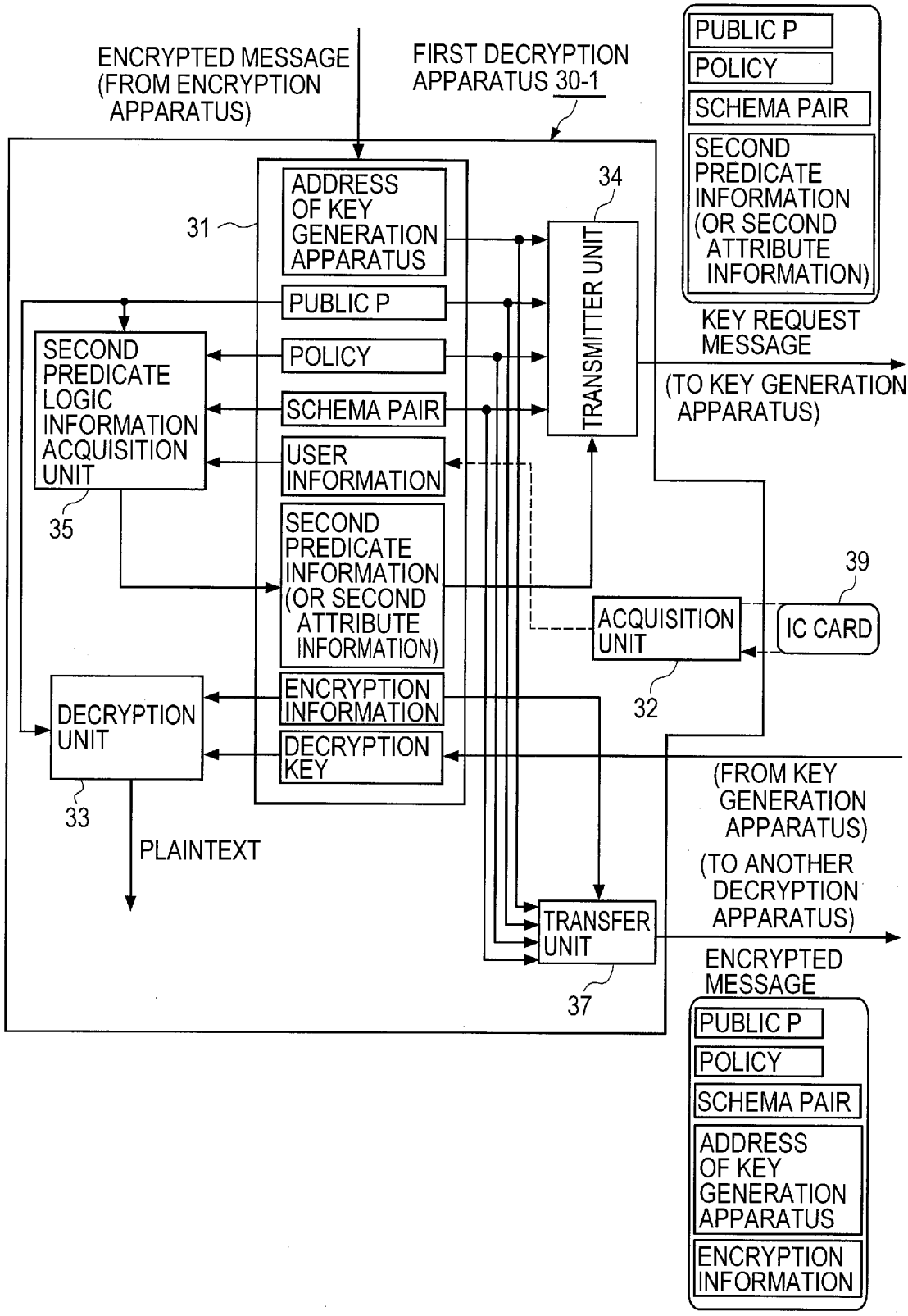

ENCRYPTED MESSAGE (FROM ENCRYPTION APPARATUS)
FIRST DECRYPTION APPARATUS 30-1
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
31
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
ENCRYPTION INFORMATION
DECRYPTION KEY
34
TRANSMITTER UNIT
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
39
ACQUISITION UNIT
IC CARD
32
DECRYPTION UNIT
33
PLAINTEXT
(FROM KEY GENERATION APPARATUS)
(TO ANOTHER DECRYPTION APPARATUS)
TRANSFER UNIT
37
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION

FIG.56

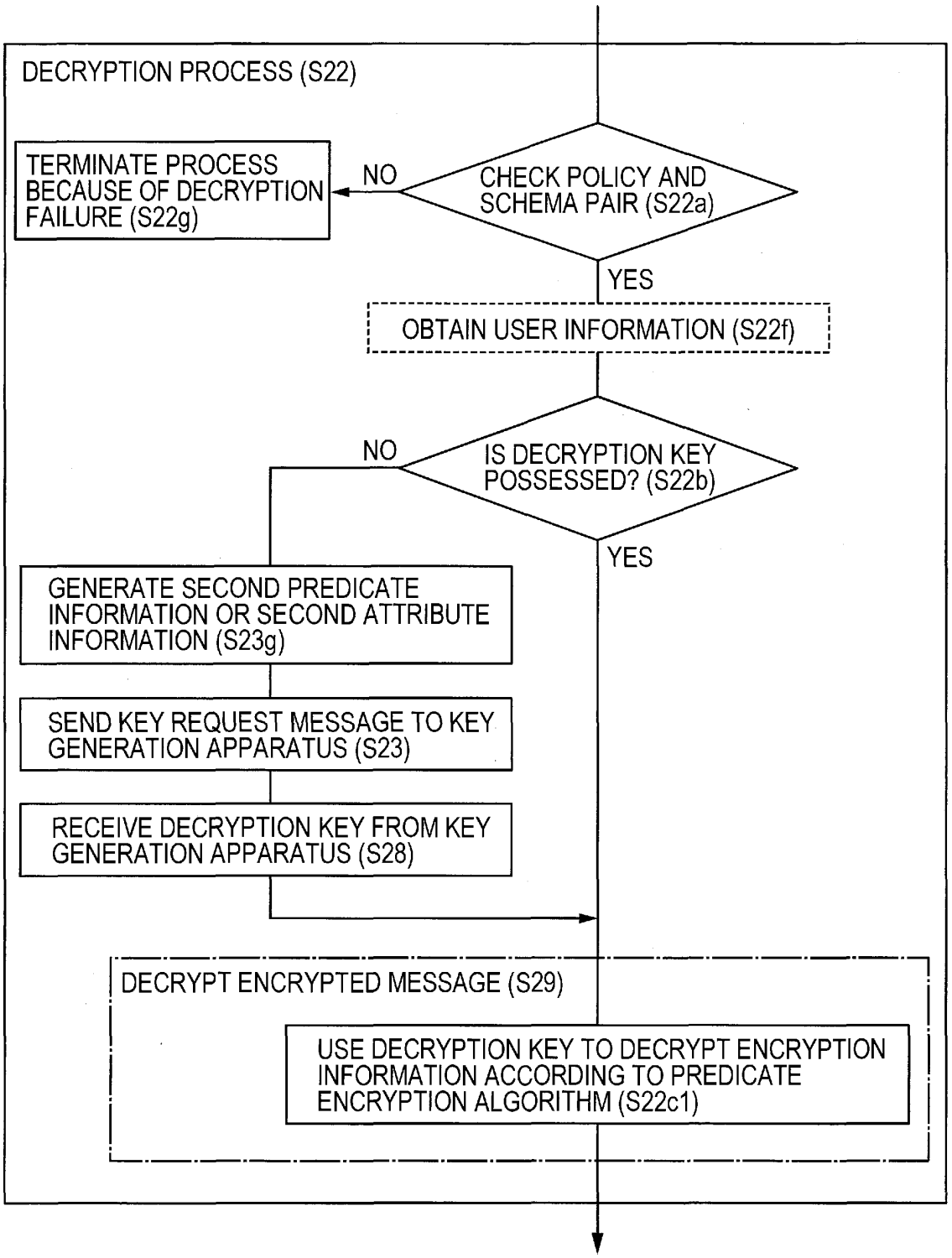

DECRYPTION PROCESS (S22)
CHECK POLICY AND SCHEMA PAIR (S22a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S22g)
YES
OBTAIN USER INFORMATION (S22f)
IS DECRYPTION KEY POSSESSED? (S22b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S23g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S23)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S28)
DECRYPT ENCRYPTED MESSAGE (S29)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S22c1)

FIG.57

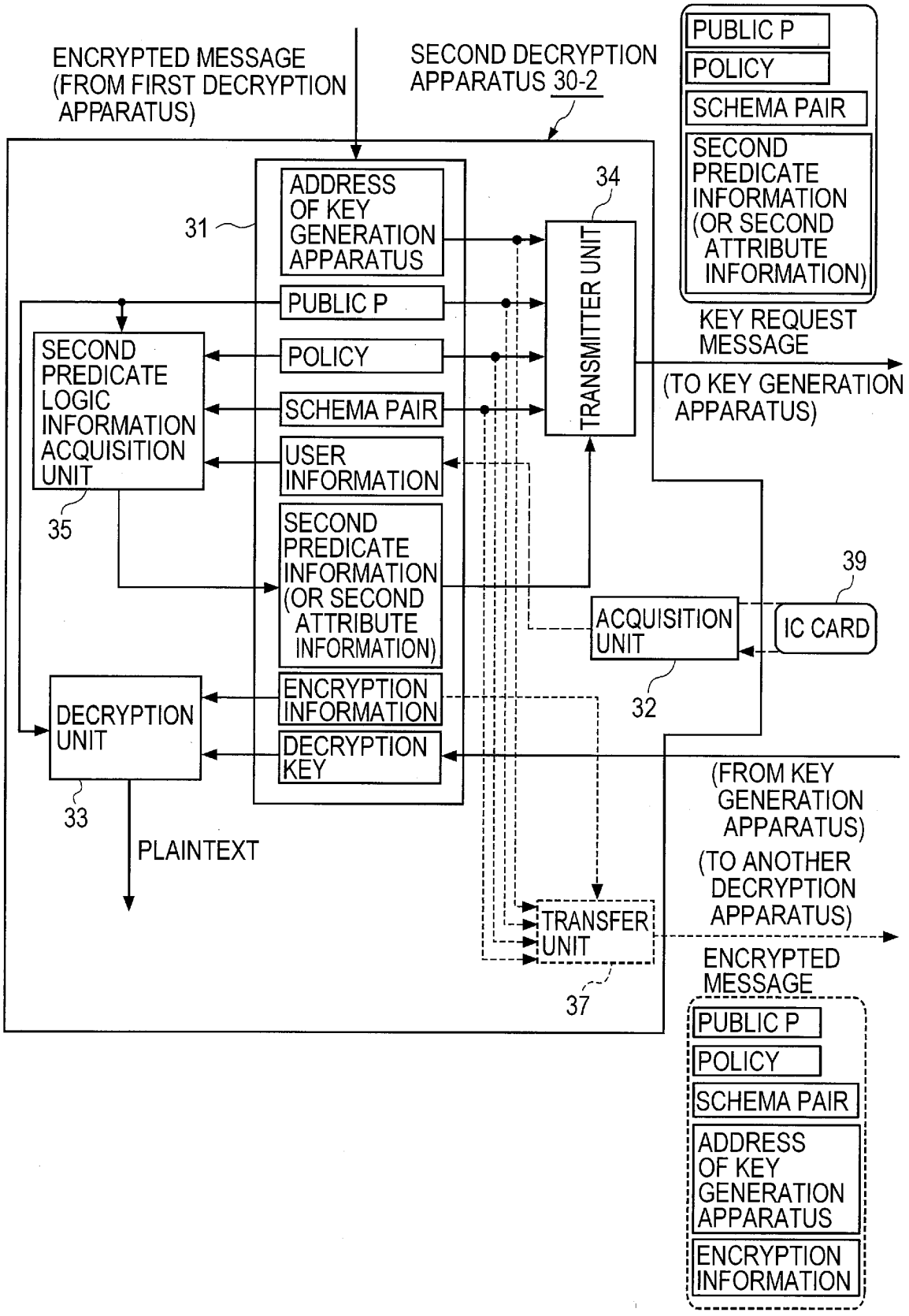

ENCRYPTED MESSAGE (FROM FIRST DECRYPTION APPARATUS)
SECOND DECRYPTION APPARATUS 30-2
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
31
ADDRESS OF KEY GENERATION APPARATUS
34
TRANSMITTER UNIT
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
39
ACQUISITION UNIT
IC CARD
32
ENCRYPTION INFORMATION
DECRYPTION KEY
DECRYPTION UNIT
33
PLAINTEXT
(FROM KEY GENERATION APPARATUS)
(TO ANOTHER DECRYPTION APPARATUS)
TRANSFER UNIT
37
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION

FIG.58

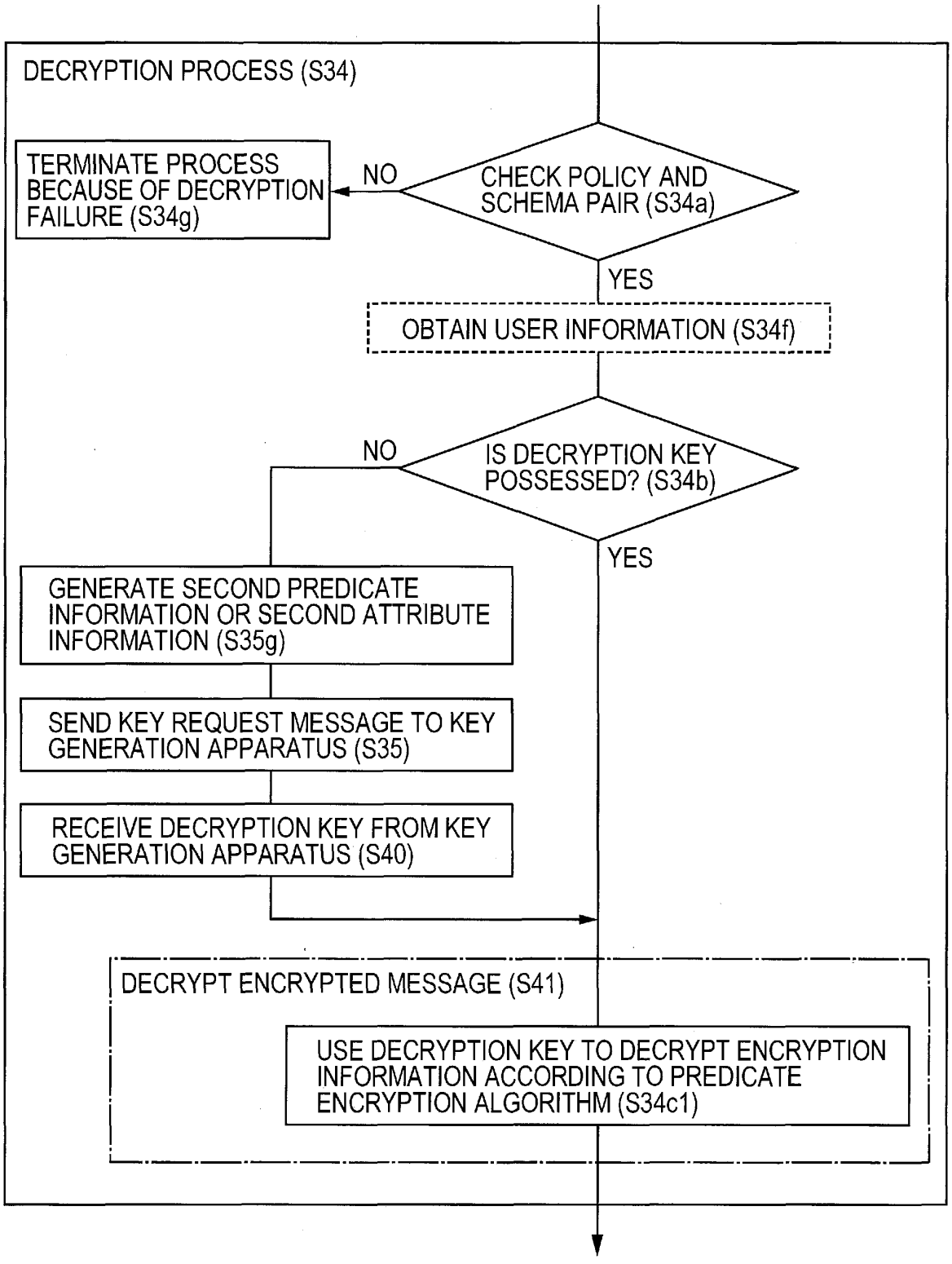

DECRYPTION PROCESS (S34)
CHECK POLICY AND SCHEMA PAIR (S34a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S34g)
YES
OBTAIN USER INFORMATION (S34f)
IS DECRYPTION KEY POSSESSED? (S34b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S35g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S35)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S40)
DECRYPT ENCRYPTED MESSAGE (S41)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S34c1)

FIG.59

S/MIME EMAIL HEADER From: ALICE TO: BOB SUBJECT:~ SENT:~
START POSITION MARKER FOR ENCRYPTED MESSAGE
ALGORITHM IDENTIFIER BLOCK - PREDICATE ENCRYPTION ALGORITHM FOR PRIVATE KEY - PRIVATE KEY ENCRYPTION ALGORITHM FOR MESSAGE PAYLOAD
DIGITAL SIGNATURE BLOCK
PUBLIC PARAMETER INFORMATION BLOCK
POLICY FIELD
SCHEMA FIELD
ENCRYPTION INFORMATION FIELD
CIPHERTEXT FIELD
ATTRIBUTE FIELD
PREDICATE FIELD
END POSITION MARKER FOR ENCRYPTED MESSAGE
ATTACHMENT FIELD (RSA ENCRYPTION ATTACHMENT, FOR EXAMPLE)

FIG.60

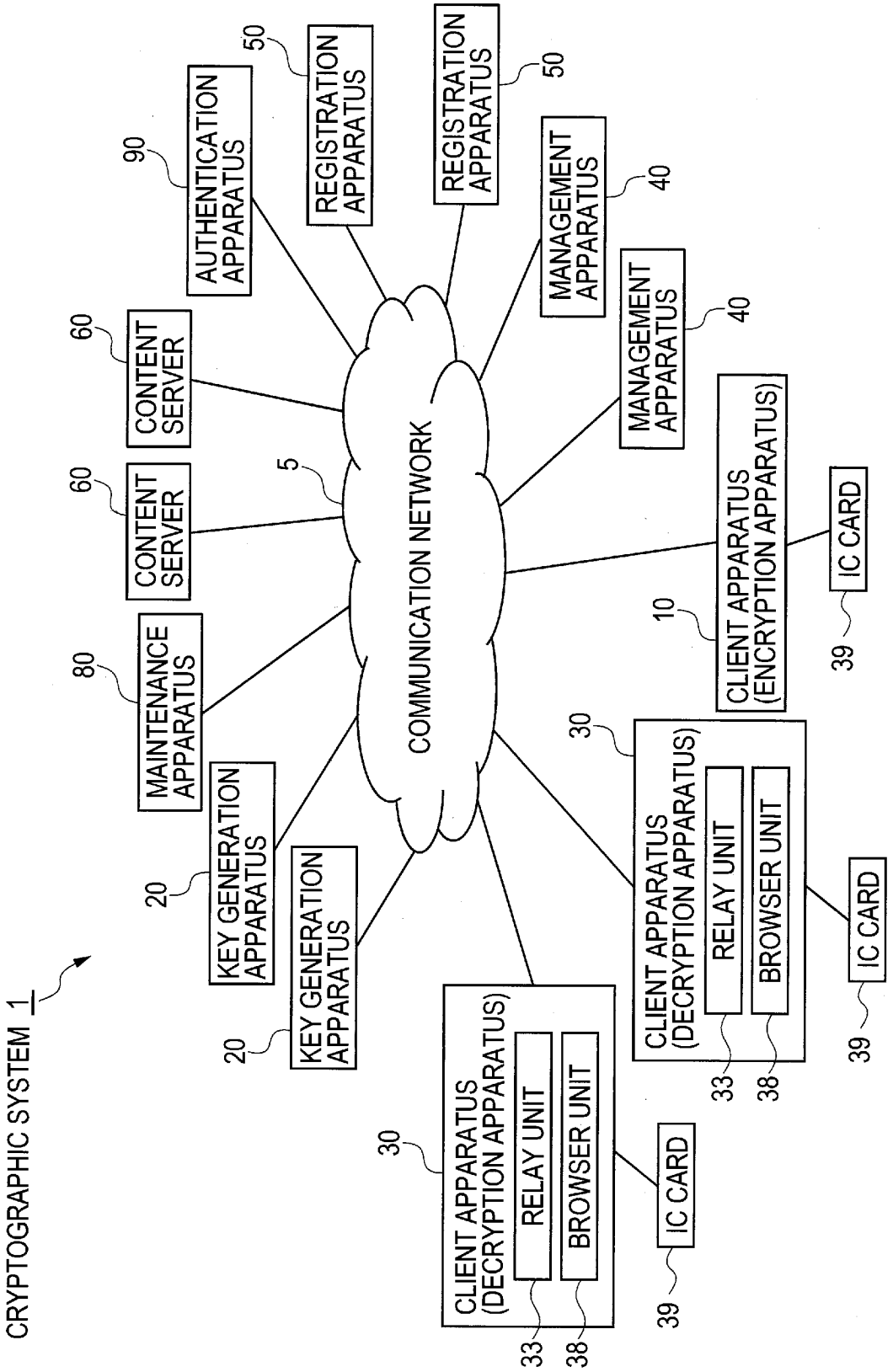

CRYPTOGRAPHIC SYSTEM 1
COMMUNICATION NETWORK
5
AUTHENTICATION APPARATUS
90
REGISTRATION APPARATUS
50
REGISTRATION APPARATUS
50
MANAGEMENT APPARATUS
40
MANAGEMENT APPARATUS
40
CONTENT SERVER
60
CONTENT SERVER
60
MAINTENANCE APPARATUS
80
KEY GENERATION APPARATUS
20
KEY GENERATION APPARATUS
20
CLIENT APPARATUS (ENCRYPTION APPARATUS)
10
IC CARD
39
CLIENT APPARATUS (DECRYPTION APPARATUS)
30
RELAY UNIT
33
BROWSER UNIT
38
IC CARD
39
CLIENT APPARATUS (DECRYPTION APPARATUS)
30
RELAY UNIT
33
BROWSER UNIT
38
IC CARD
39

FIG.61

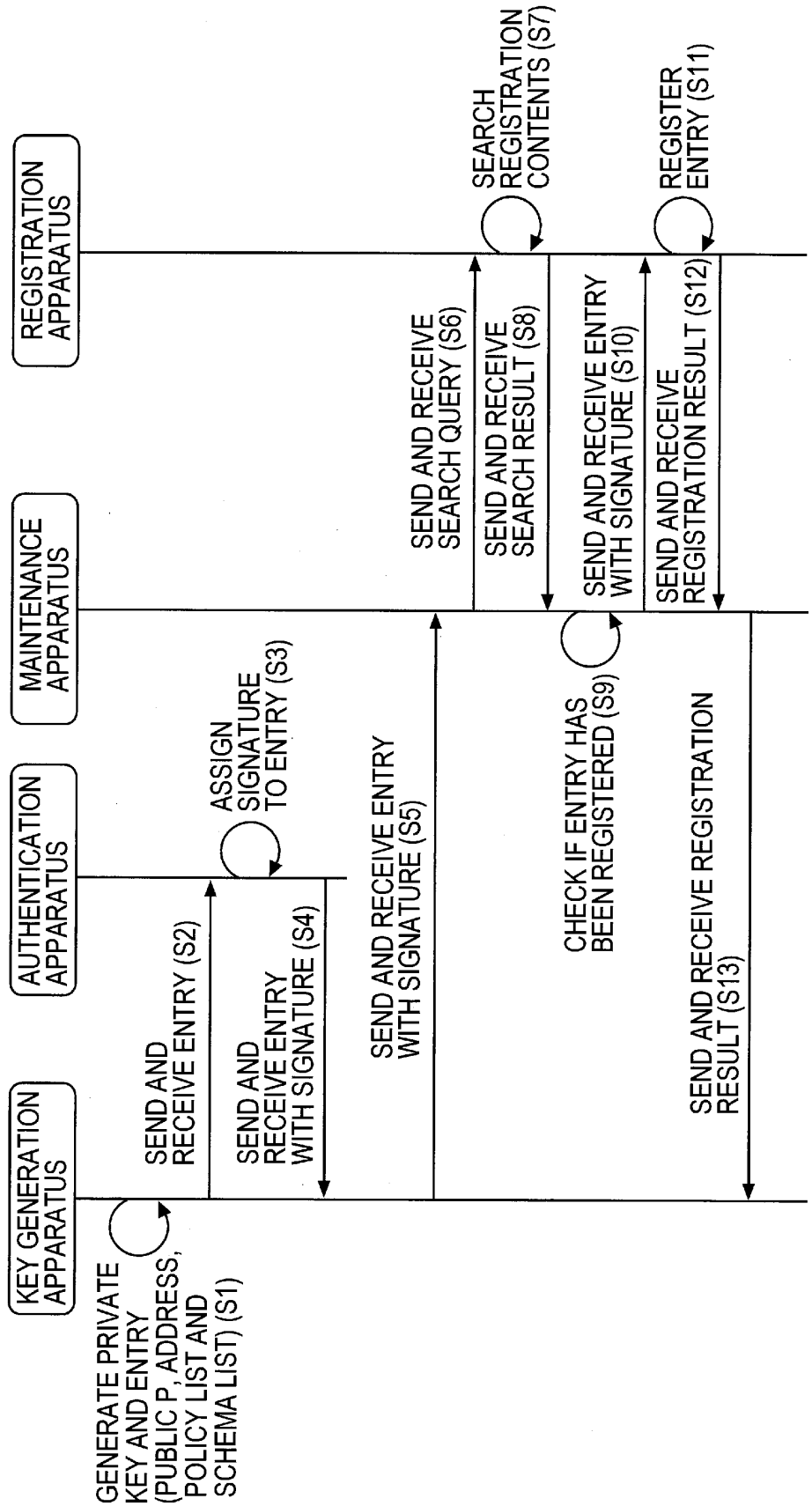

KEY GENERATION APPARATUS
AUTHENTICATION APPARATUS
MAINTENANCE APPARATUS
REGISTRATION APPARATUS
GENERATE PRIVATE KEY AND ENTRY (PUBLIC P, ADDRESS, POLICY LIST AND SCHEMA LIST) (S1)
SEND AND RECEIVE ENTRY (S2)
ASSIGN SIGNATURE TO ENTRY (S3)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S4)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S5)
SEND AND RECEIVE SEARCH QUERY (S6)
SEARCH REGISTRATION CONTENTS (S7)
SEND AND RECEIVE SEARCH RESULT (S8)
CHECK IF ENTRY HAS BEEN REGISTERED (S9)
SEND AND RECEIVE ENTRY WITH SIGNATURE (S10)
REGISTER ENTRY (S11)
SEND AND RECEIVE REGISTRATION RESULT (S12)
SEND AND RECEIVE REGISTRATION RESULT (S13)

FIG.62

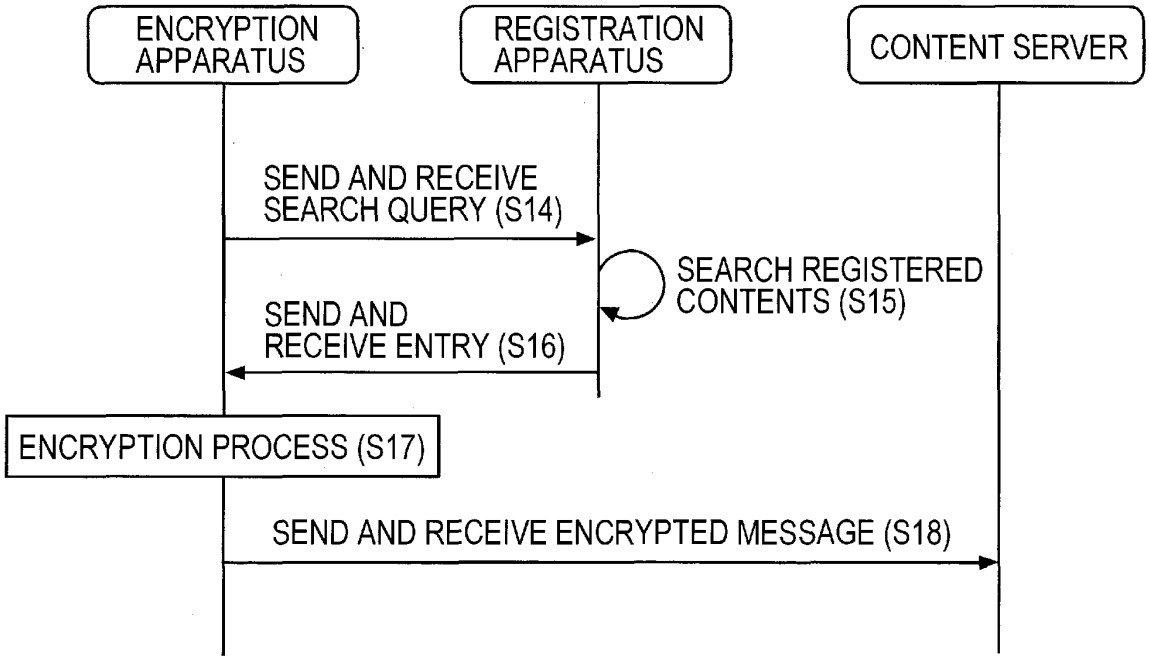
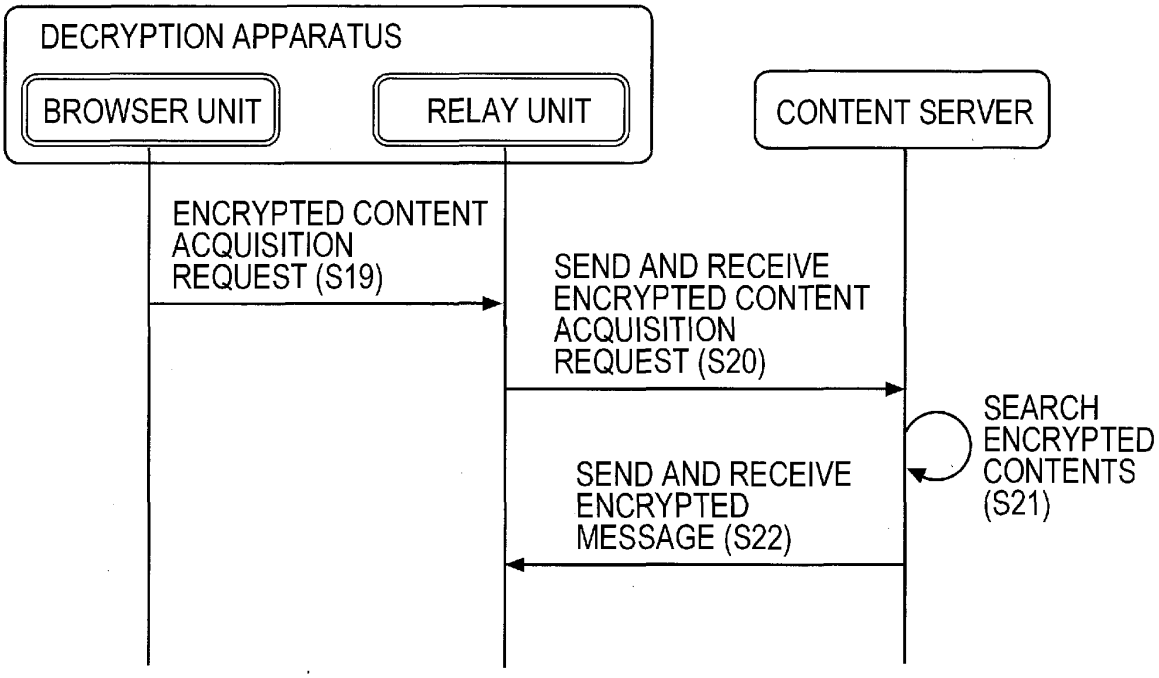

ENCRYPTION APPARATUS
REGISTRATION APPARATUS
CONTENT SERVER
SEND AND RECEIVE SEARCH QUERY (S14)
SEARCH REGISTERED CONTENTS (S15)
SEND AND RECEIVE ENTRY (S16)
ENCRYPTION PROCESS (S17)
SEND AND RECEIVE ENCRYPTED MESSAGE (S18)

FIG.63


DECRYPTION APPARATUS
BROWSER UNIT
RELAY UNIT
CONTENT SERVER
ENCRYPTED CONTENT ACQUISITION REQUEST (S19)
SEND AND RECEIVE ENCRYPTED CONTENT ACQUISITION REQUEST (S20)
SEARCH ENCRYPTED CONTENTS (S21)
SEND AND RECEIVE ENCRYPTED MESSAGE (S22)

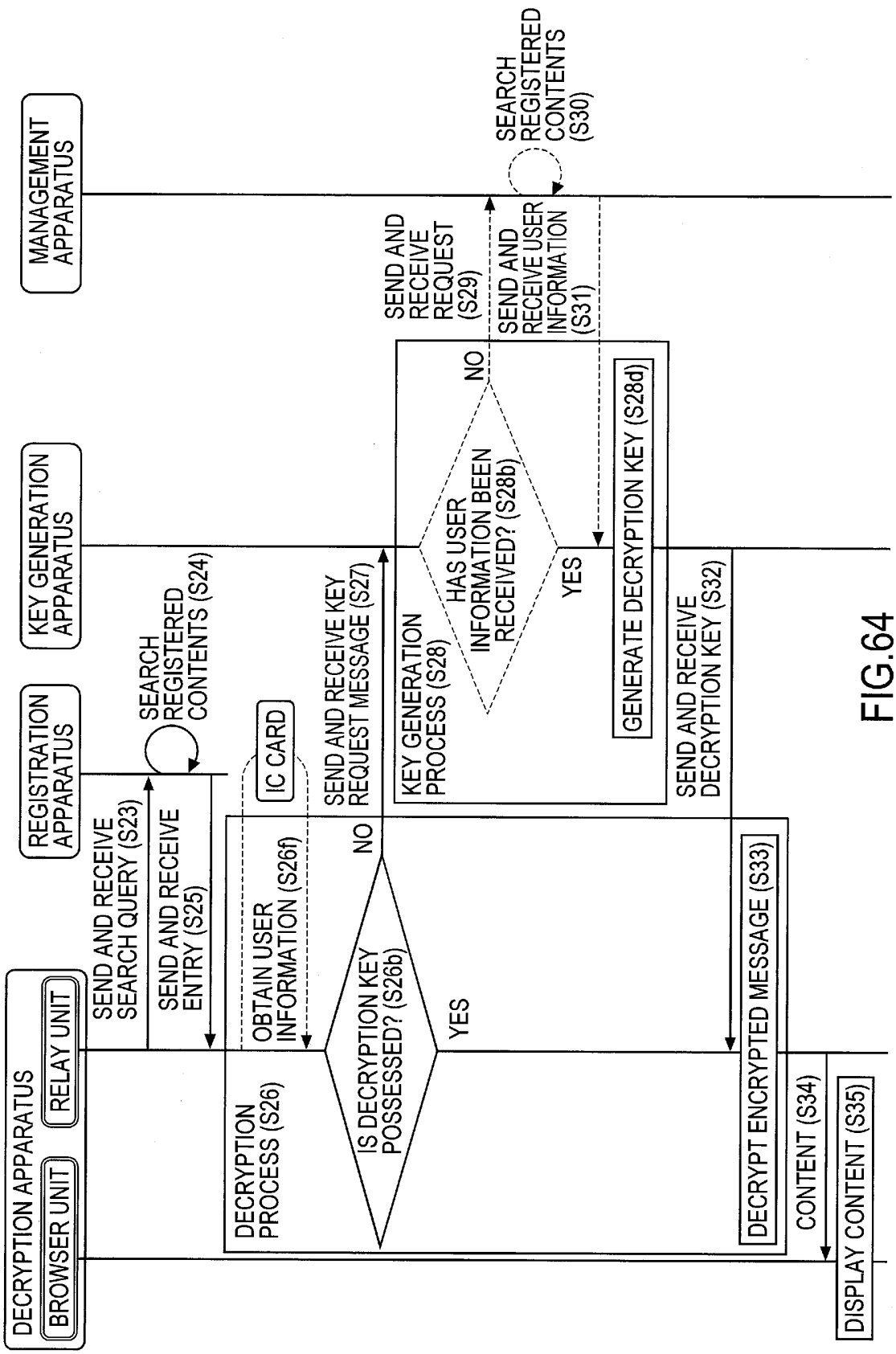

DECRYPTION APPARATUS
BROWSER UNIT
RELAY UNIT
REGISTRATION APPARATUS
KEY GENERATION APPARATUS
MANAGEMENT APPARATUS
SEND AND RECEIVE SEARCH QUERY (S23)
SEARCH REGISTERED CONTENTS (S24)
SEND AND RECEIVE ENTRY (S25)
DECRYPTION PROCESS (S26)
IC CARD
OBTAIN USER INFORMATION (S26f)
IS DECRYPTION KEY POSSESSED? (S26b)
NO
YES
SEND AND RECEIVE KEY REQUEST MESSAGE (S27)
KEY GENERATION PROCESS (S28)
HAS USER INFORMATION BEEN RECEIVED? (S28b)
NO
YES
SEND AND RECEIVE REQUEST (S29)
SEARCH REGISTERED CONTENTS (S30)
SEND AND RECEIVE USER INFORMATION (S31)
GENERATE DECRYPTION KEY (S28d)
SEND AND RECEIVE DECRYPTION KEY (S32)
DECRYPT ENCRYPTED MESSAGE (S33)
CONTENT (S34)
DISPLAY CONTENT (S35)

FIG.64

FIG.65

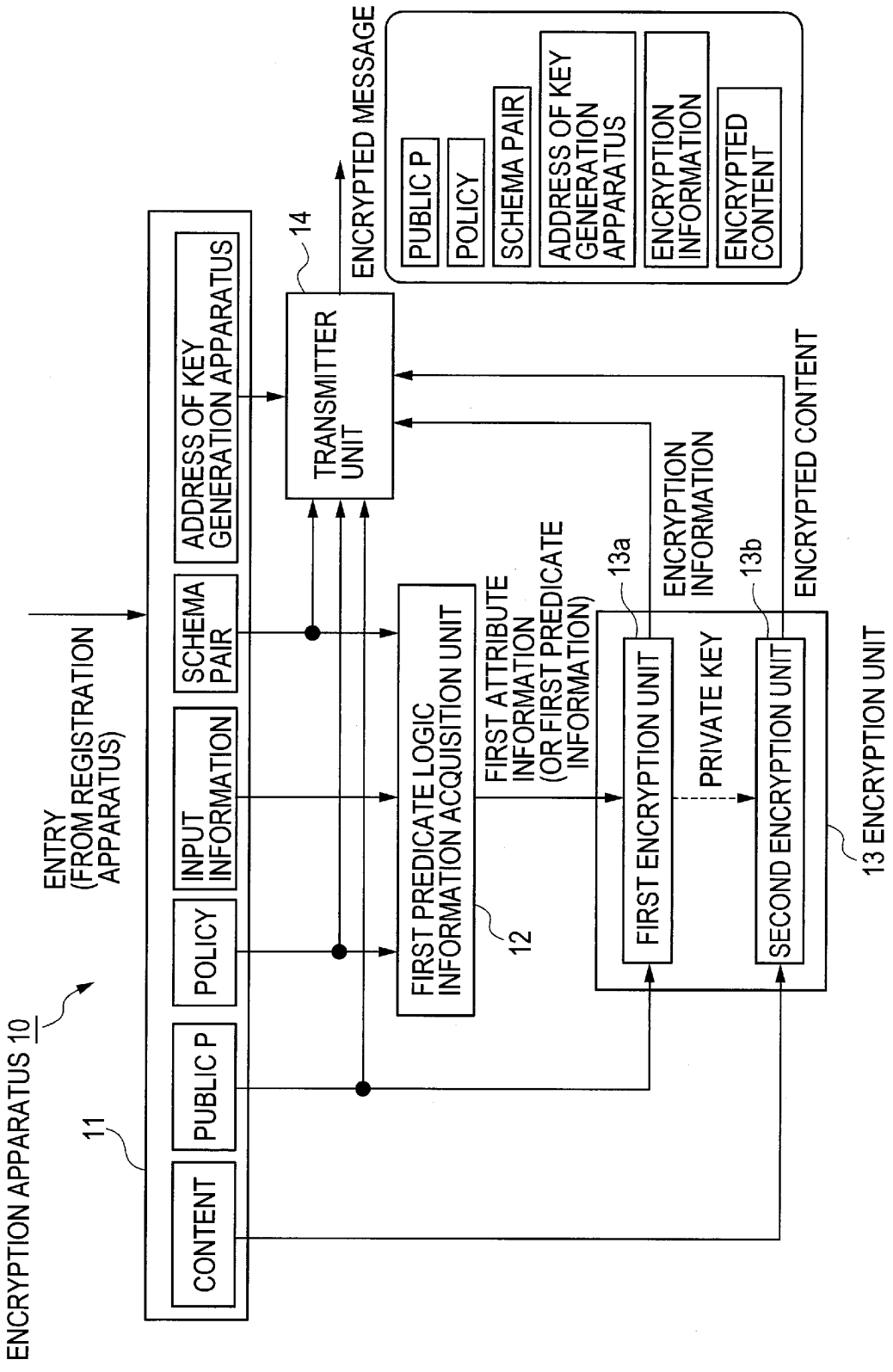

ENCRYPTION APPARATUS 10
ENTRY (FROM REGISTRATION APPARATUS)
11
CONTENT
PUBLIC P
POLICY
INPUT INFORMATION
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
FIRST PREDICATE LOGIC INFORMATION ACQUISITION UNIT
12
FIRST ATTRIBUTE INFORMATION (OR FIRST PREDICATE INFORMATION)
TRANSMITTER UNIT
14
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTION INFORMATION
ENCRYPTED CONTENT
13a
FIRST ENCRYPTION UNIT
ENCRYPTION INFORMATION
PRIVATE KEY
13b
SECOND ENCRYPTION UNIT
ENCRYPTED CONTENT
13 ENCRYPTION UNIT

FIG.66

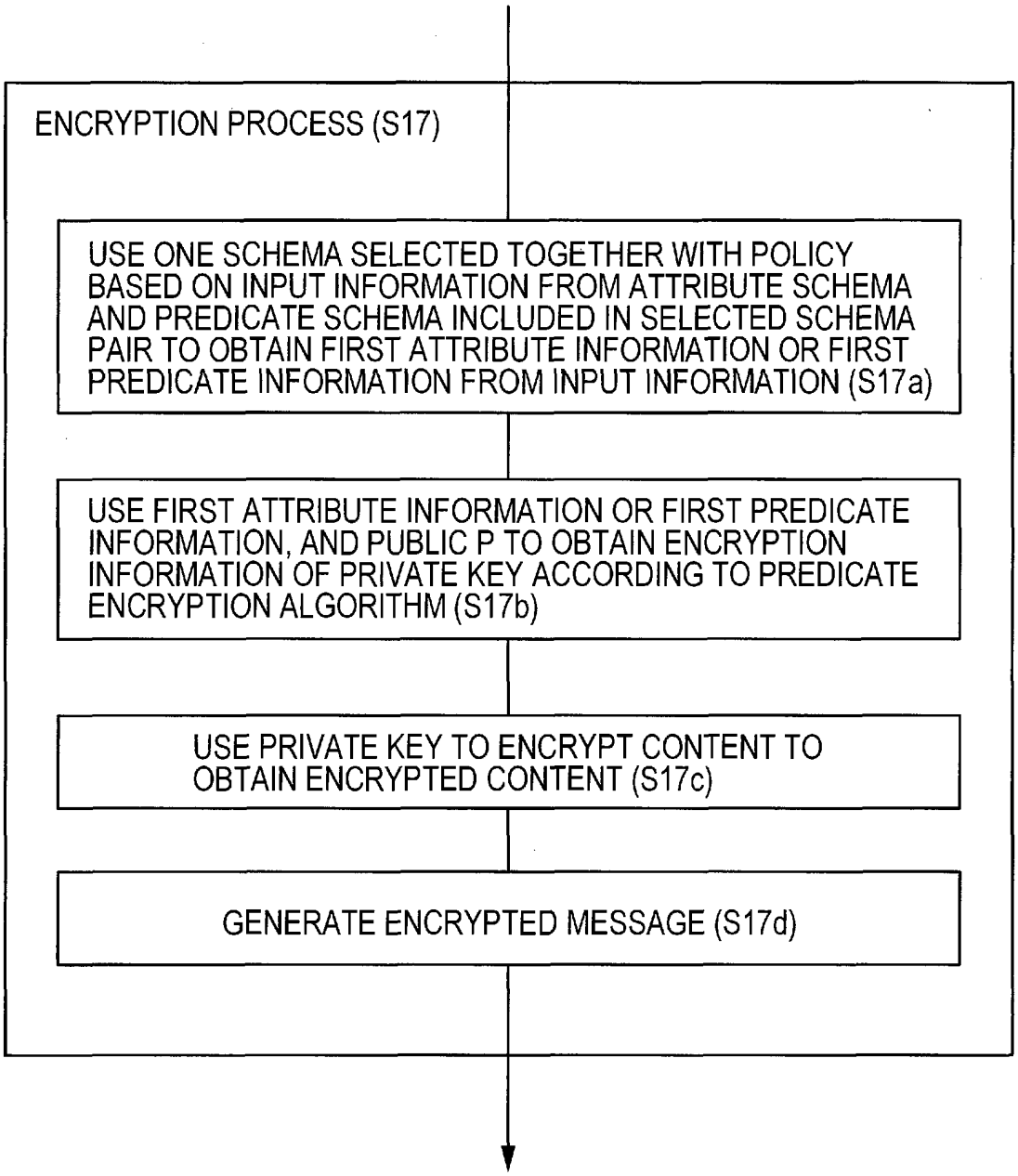

ENCRYPTION PROCESS (S17)
USE ONE SCHEMA SELECTED TOGETHER WITH POLICY BASED ON INPUT INFORMATION FROM ATTRIBUTE SCHEMA AND PREDICATE SCHEMA INCLUDED IN SELECTED SCHEMA PAIR TO OBTAIN FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION FROM INPUT INFORMATION (S17a)
USE FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION, AND PUBLIC P TO OBTAIN ENCRYPTION INFORMATION OF PRIVATE KEY ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S17b)
USE PRIVATE KEY TO ENCRYPT CONTENT TO OBTAIN ENCRYPTED CONTENT (S17c)
GENERATE ENCRYPTED MESSAGE (S17d)

FIG.67

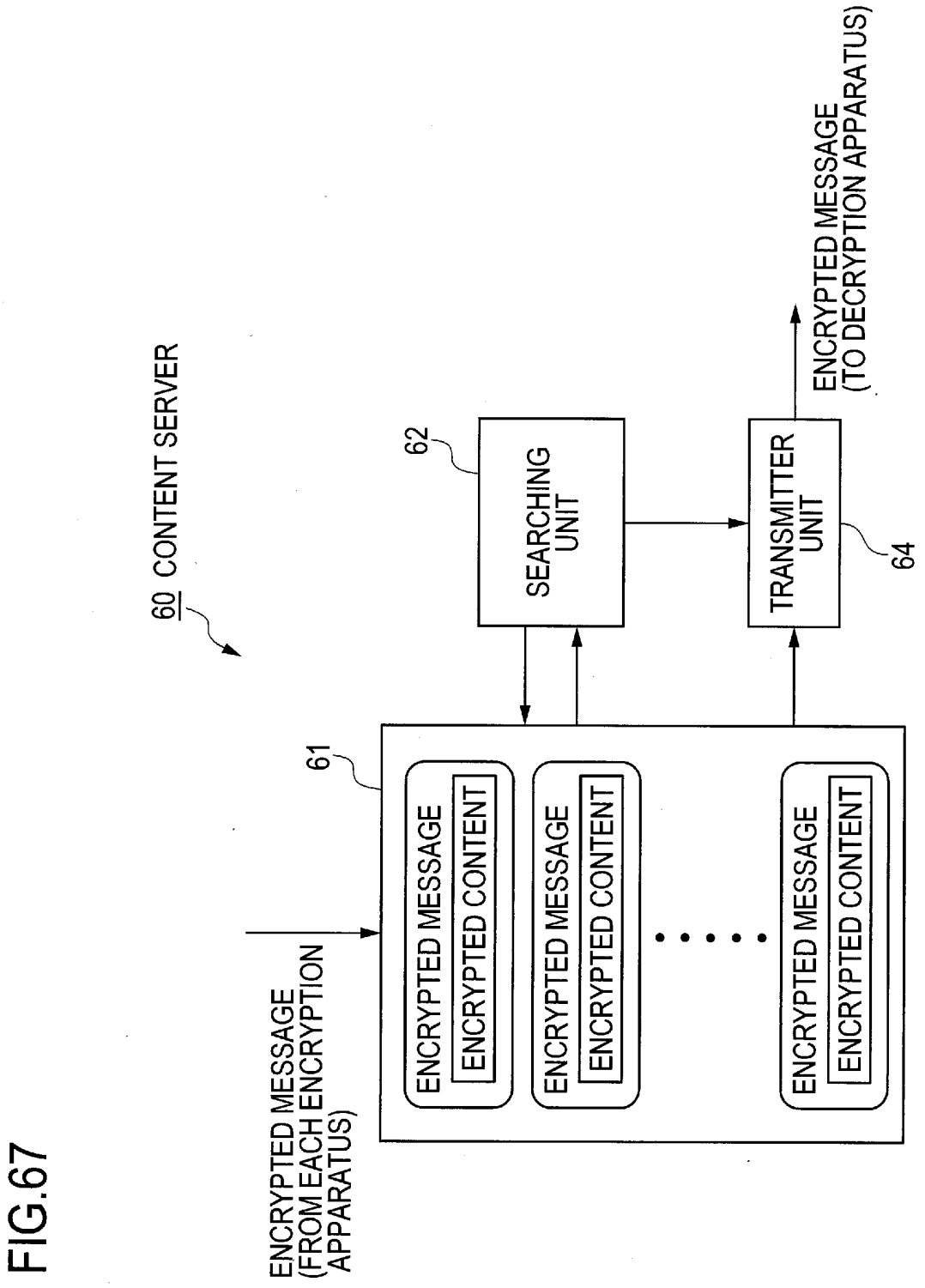

60 CONTENT SERVER
61
62
SEARCHING UNIT
TRANSMITTER UNIT
64
ENCRYPTED MESSAGE (TO DECRYPTION APPARATUS)
ENCRYPTED MESSAGE (FROM EACH ENCRYPTION APPARATUS)
ENCRYPTED MESSAGE
ENCRYPTED CONTENT
ENCRYPTED MESSAGE
ENCRYPTED CONTENT
ENCRYPTED MESSAGE
ENCRYPTED CONTENT

FIG.68

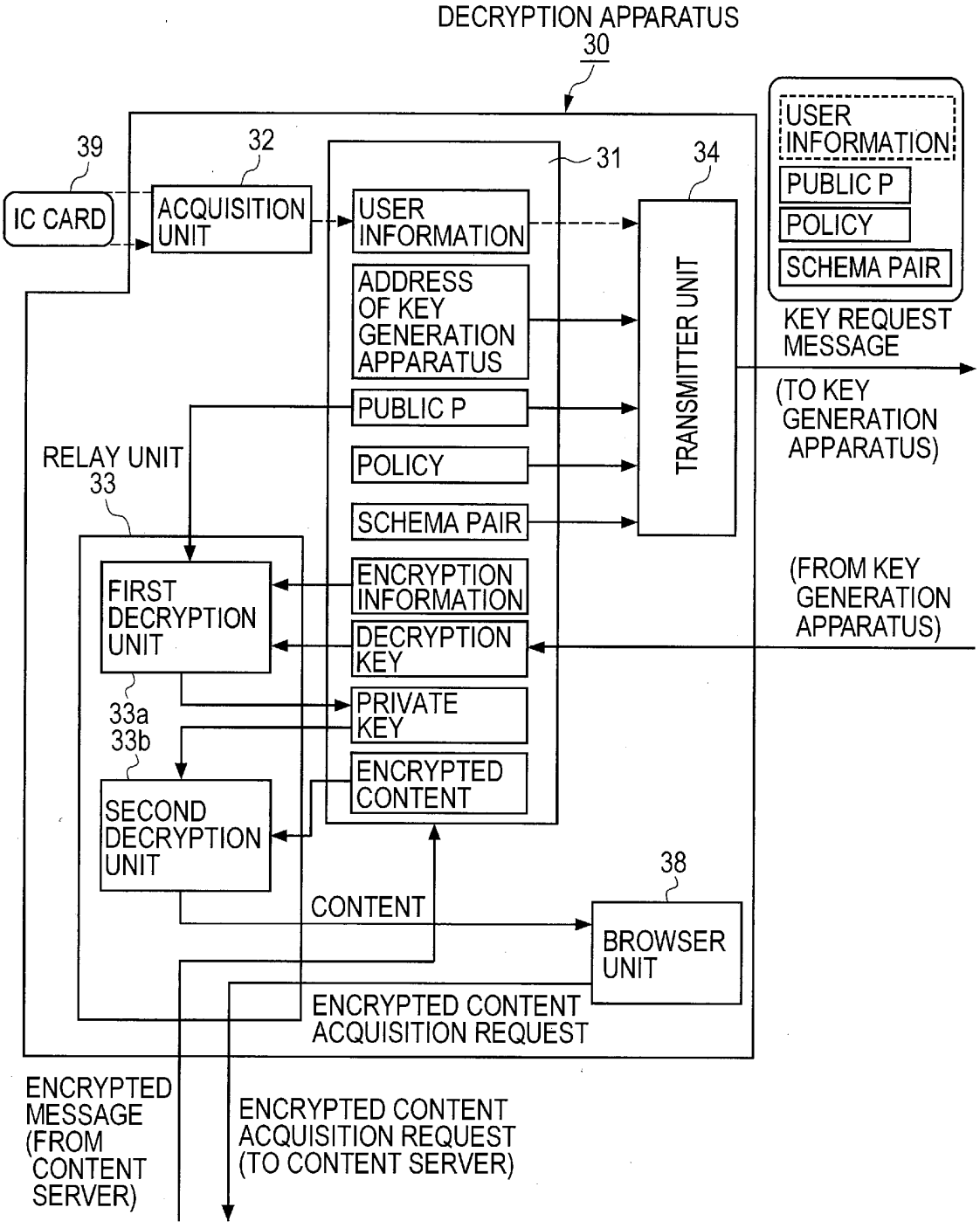

DECRYPTION APPARATUS
30
39
IC CARD
32
ACQUISITION UNIT
31
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
34
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
RELAY UNIT
33
FIRST DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
(FROM KEY GENERATION APPARATUS)
33a
33b
PRIVATE KEY
ENCRYPTED CONTENT
SECOND DECRYPTION UNIT
38
CONTENT
BROWSER UNIT
ENCRYPTED CONTENT ACQUISITION REQUEST
ENCRYPTED MESSAGE (FROM CONTENT SERVER)
ENCRYPTED CONTENT ACQUISITION REQUEST (TO CONTENT SERVER)

FIG.69

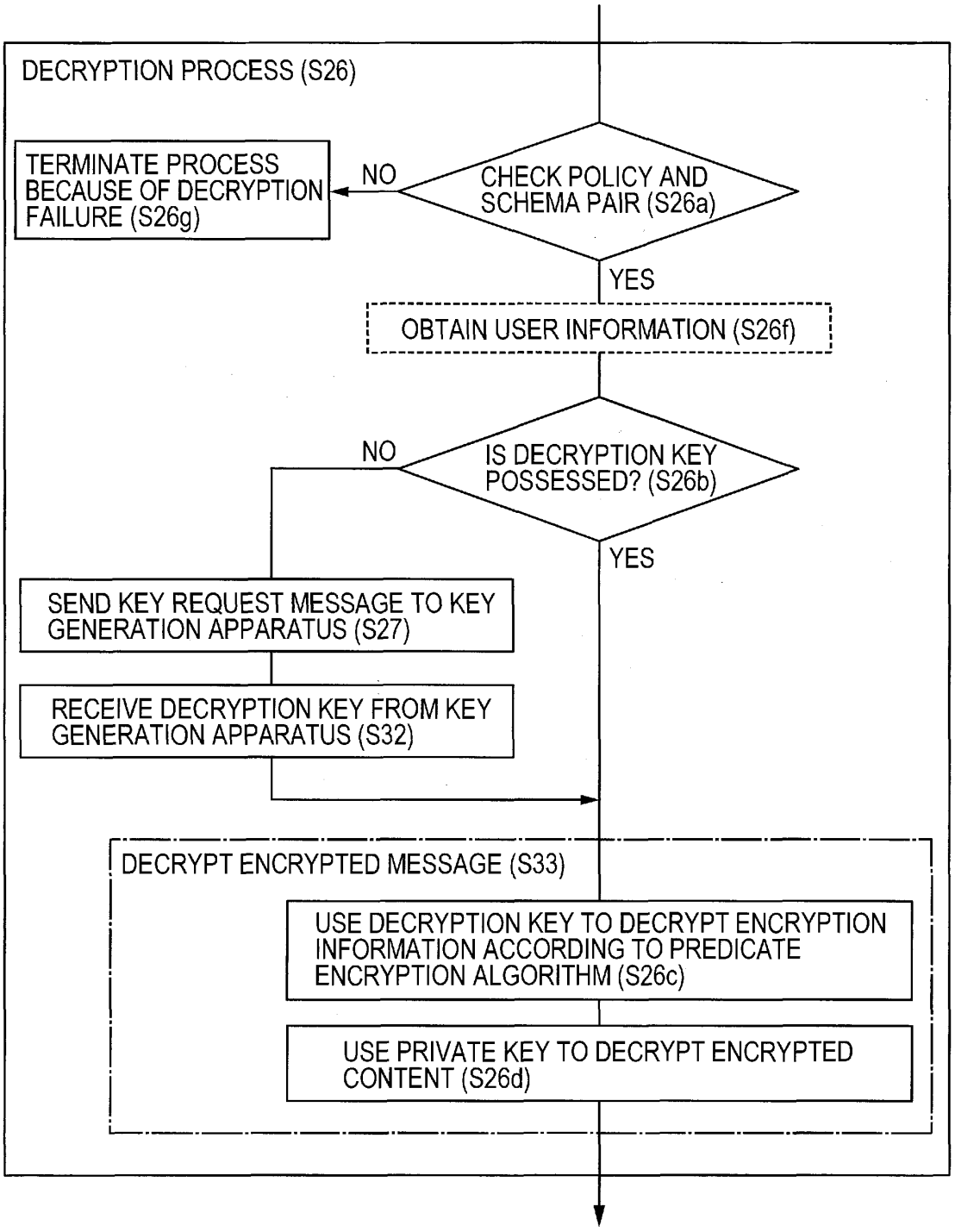

DECRYPTION PROCESS (S26)
CHECK POLICY AND SCHEMA PAIR (S26a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S26g)
YES
OBTAIN USER INFORMATION (S26f)
IS DECRYPTION KEY POSSESSED? (S26b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S27)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S32)
DECRYPT ENCRYPTED MESSAGE (S33)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S26c)
USE PRIVATE KEY TO DECRYPT ENCRYPTED CONTENT (S26d)

FIG.70

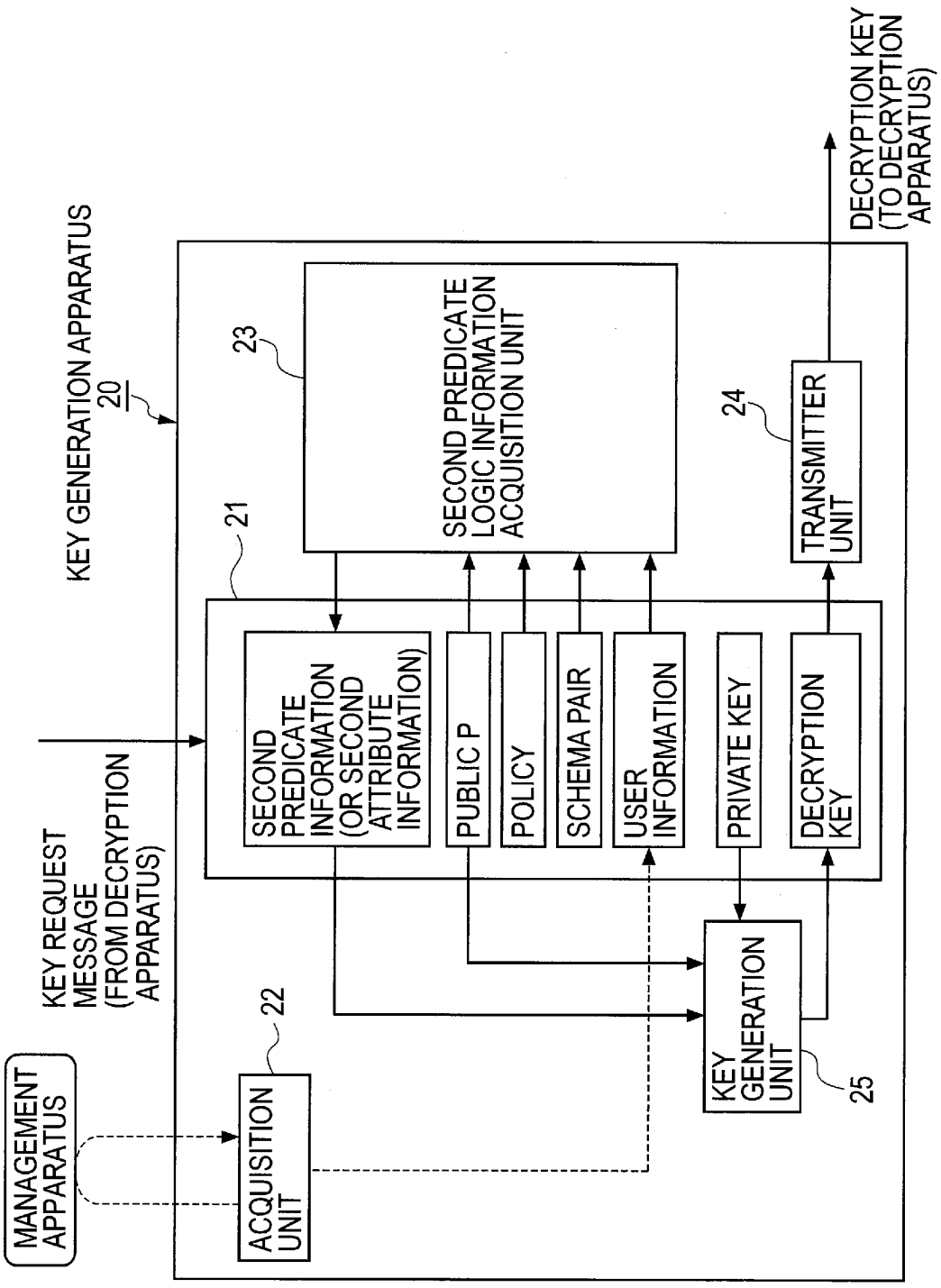

KEY GENERATION APPARATUS
20
KEY REQUEST MESSAGE (FROM DECRYPTION APPARATUS)
MANAGEMENT APPARATUS
ACQUISITION UNIT
22
21
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
PRIVATE KEY
DECRYPTION KEY
23
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
24
TRANSMITTER UNIT
DECRYPTION KEY (TO DECRYPTION APPARATUS)
KEY GENERATION UNIT
25

FIG.71

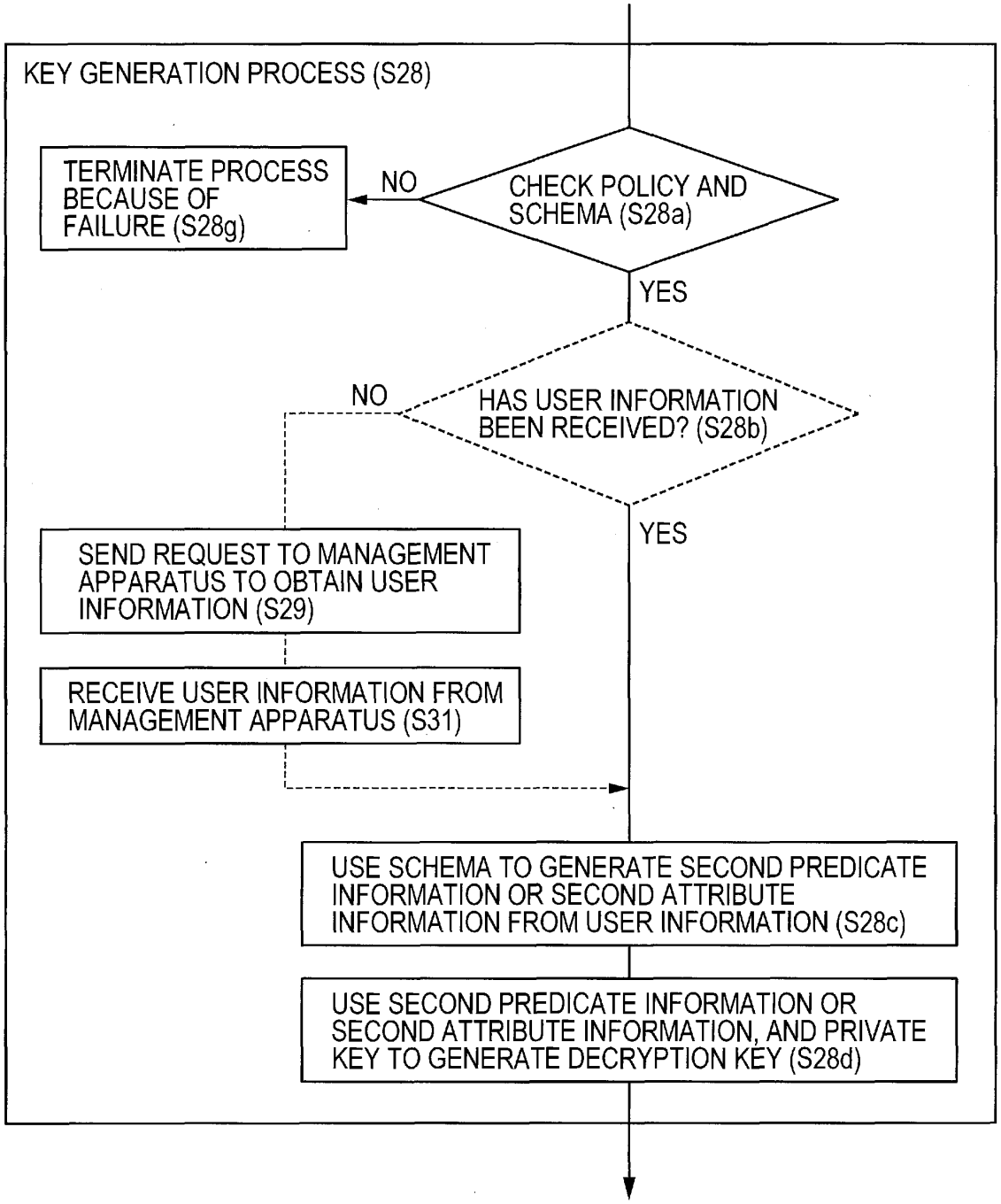

KEY GENERATION PROCESS (S28)
CHECK POLICY AND SCHEMA (S28a)
NO
TERMINATE PROCESS BECAUSE OF FAILURE (S28g)
YES
HAS USER INFORMATION BEEN RECEIVED? (S28b)
NO
YES
SEND REQUEST TO MANAGEMENT APPARATUS TO OBTAIN USER INFORMATION (S29)
RECEIVE USER INFORMATION FROM MANAGEMENT APPARATUS (S31)
USE SCHEMA TO GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION FROM USER INFORMATION (S28c)
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S28d)

FIG.72

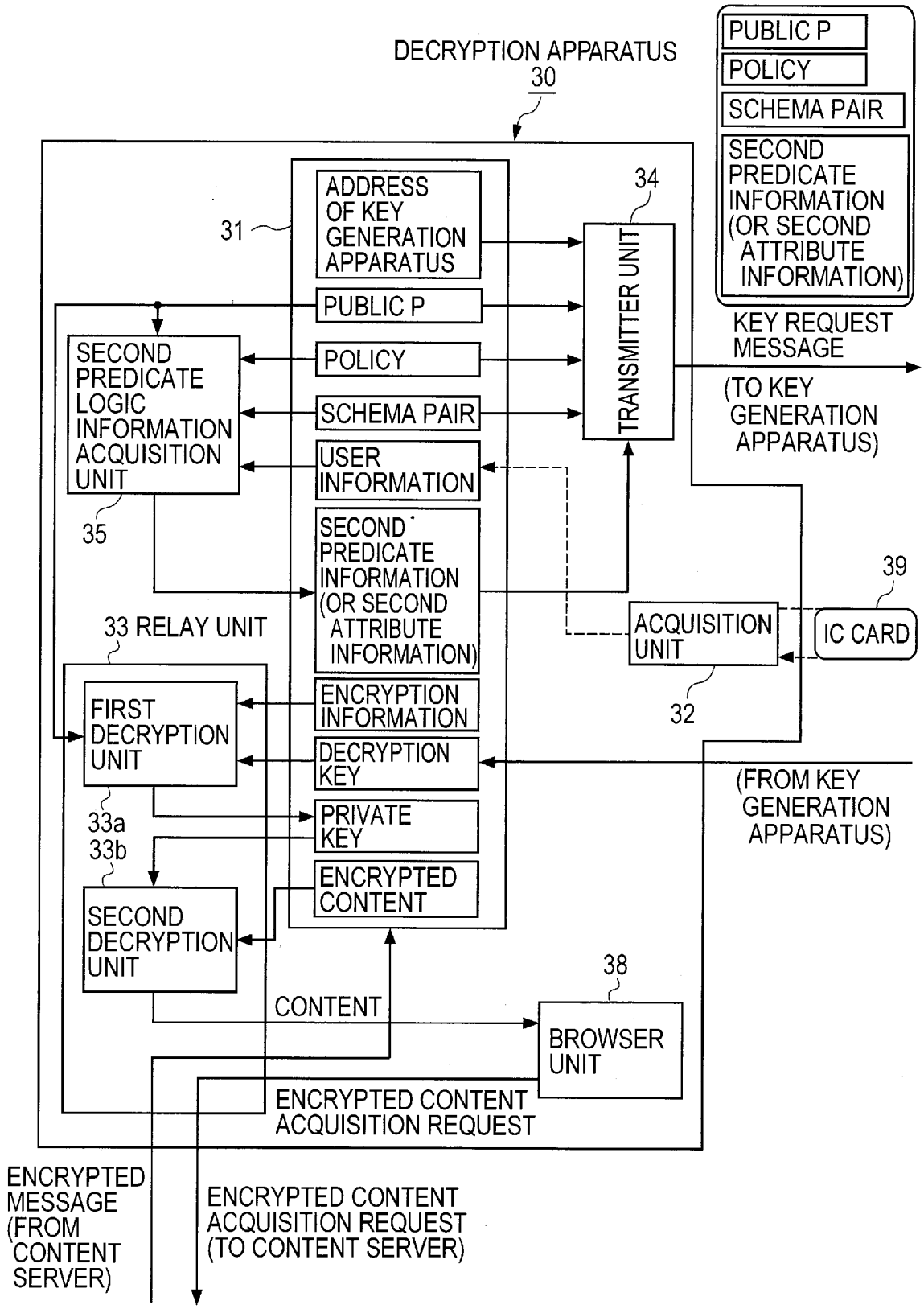

DECRYPTION APPARATUS
30
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
31
ADDRESS OF KEY GENERATION APPARATUS
34
TRANSMITTER UNIT
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
39
ACQUISITION UNIT
IC CARD
32
33 RELAY UNIT
FIRST DECRYPTION UNIT
ENCRYPTION INFORMATION
DECRYPTION KEY
PRIVATE KEY
ENCRYPTED CONTENT
(FROM KEY GENERATION APPARATUS)
33a
33b
SECOND DECRYPTION UNIT
38
CONTENT
BROWSER UNIT
ENCRYPTED CONTENT ACQUISITION REQUEST
ENCRYPTED MESSAGE (FROM CONTENT SERVER)
ENCRYPTED CONTENT ACQUISITION REQUEST (TO CONTENT SERVER)

FIG.73

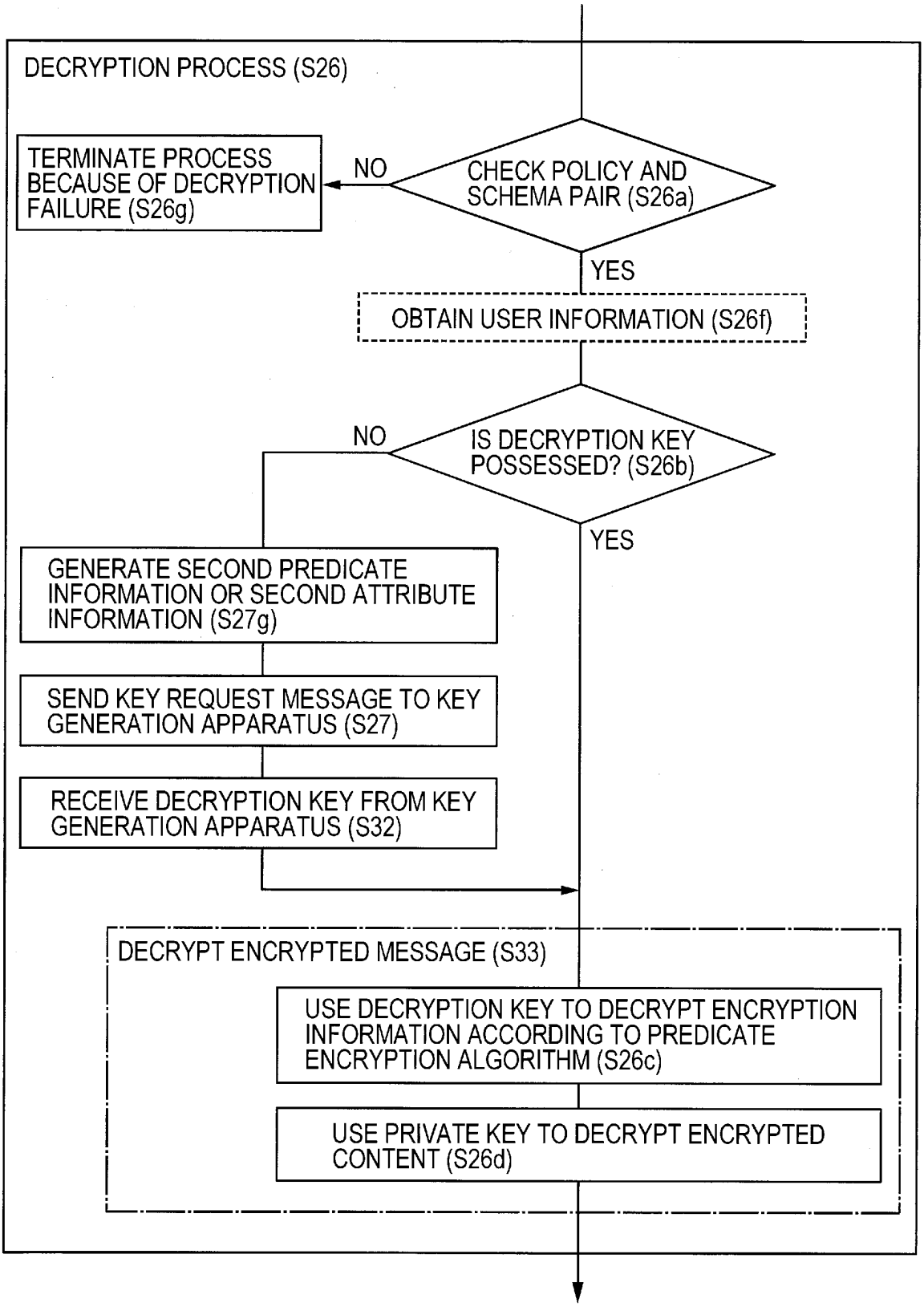

DECRYPTION PROCESS (S26)
CHECK POLICY AND SCHEMA PAIR (S26a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S26g)
YES
OBTAIN USER INFORMATION (S26f)
IS DECRYPTION KEY POSSESSED? (S26b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S27g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S27)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S32)
DECRYPT ENCRYPTED MESSAGE (S33)
USE DECRYPTION KEY TO DECRYPT ENCRYPTION INFORMATION ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S26c)
USE PRIVATE KEY TO DECRYPT ENCRYPTED CONTENT (S26d)

FIG.74

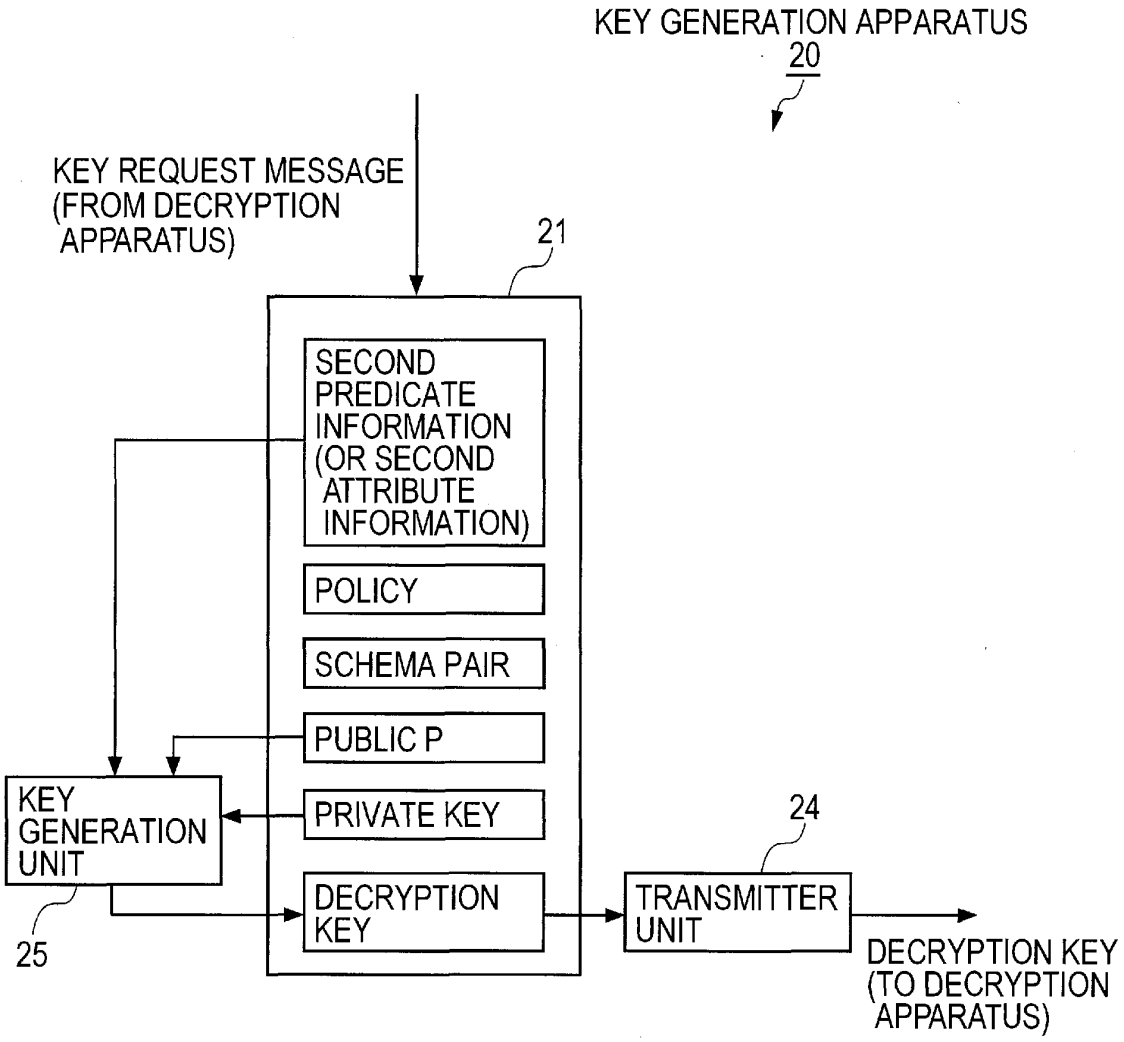

KEY GENERATION APPARATUS
20
KEY REQUEST MESSAGE (FROM DECRYPTION APPARATUS)
21
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
POLICY
SCHEMA PAIR
PUBLIC P
PRIVATE KEY
DECRYPTION KEY
KEY GENERATION UNIT
25
24
TRANSMITTER UNIT
DECRYPTION KEY (TO DECRYPTION APPARATUS)

FIG.75

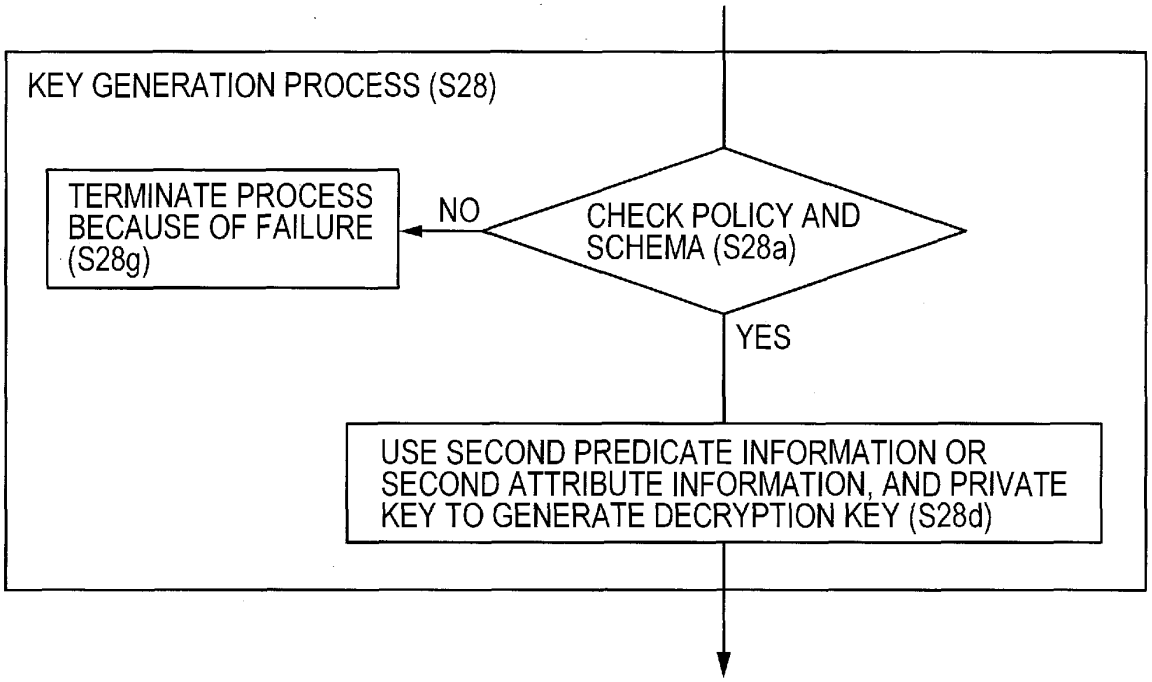

KEY GENERATION PROCESS (S28)
CHECK POLICY AND SCHEMA (S28a)
NO
TERMINATE PROCESS BECAUSE OF FAILURE (S28g)
YES
USE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION, AND PRIVATE KEY TO GENERATE DECRYPTION KEY (S28d)

FIG.76

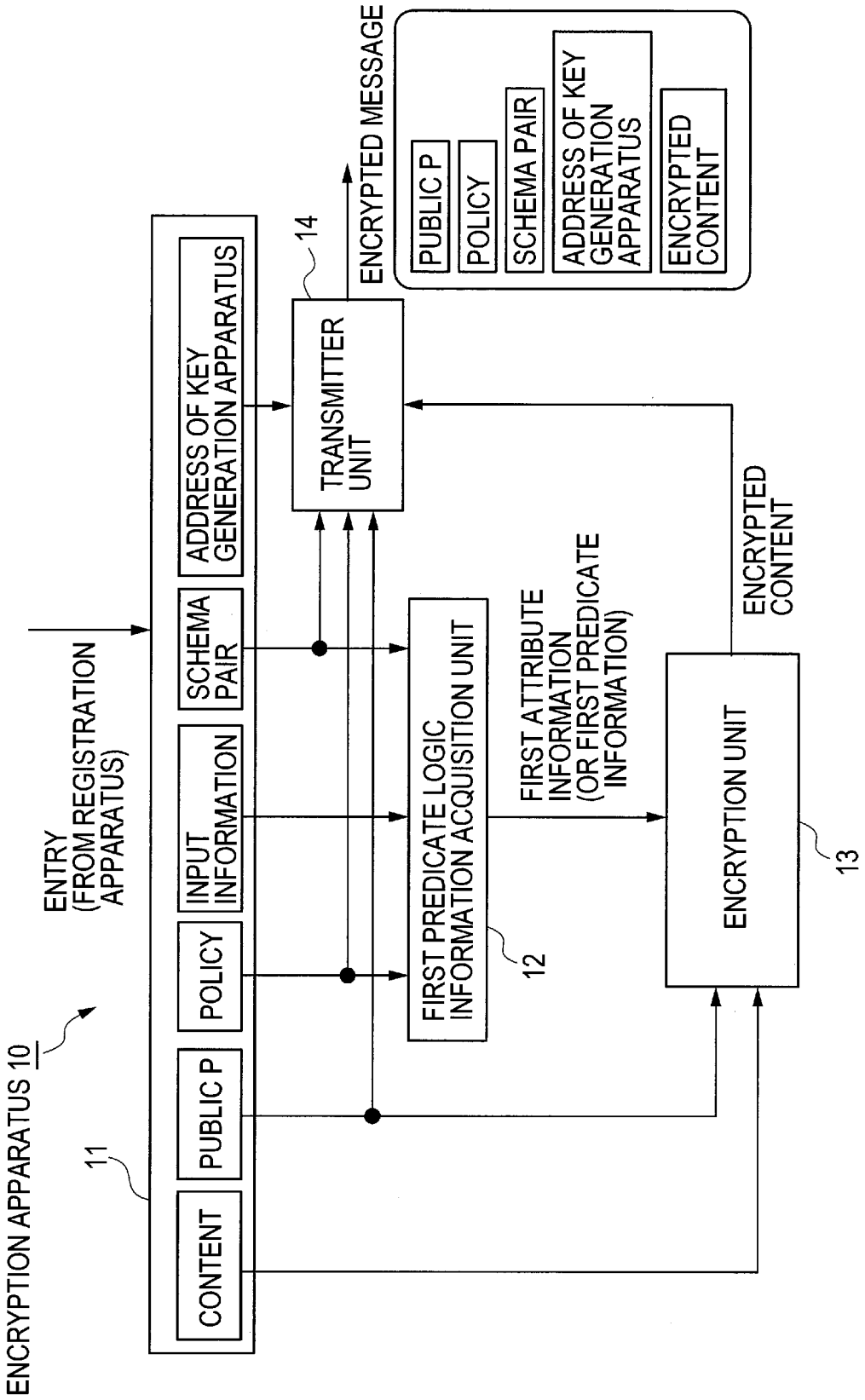

ENCRYPTION APPARATUS 10
ENTRY (FROM REGISTRATION APPARATUS)
11
CONTENT
PUBLIC P
POLICY
INPUT INFORMATION
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
FIRST PREDICATE LOGIC INFORMATION ACQUISITION UNIT
12
FIRST ATTRIBUTE INFORMATION (OR FIRST PREDICATE INFORMATION)
ENCRYPTION UNIT
13
ENCRYPTED CONTENT
TRANSMITTER UNIT
14
ENCRYPTED MESSAGE
PUBLIC P
POLICY
SCHEMA PAIR
ADDRESS OF KEY GENERATION APPARATUS
ENCRYPTED CONTENT

FIG.77

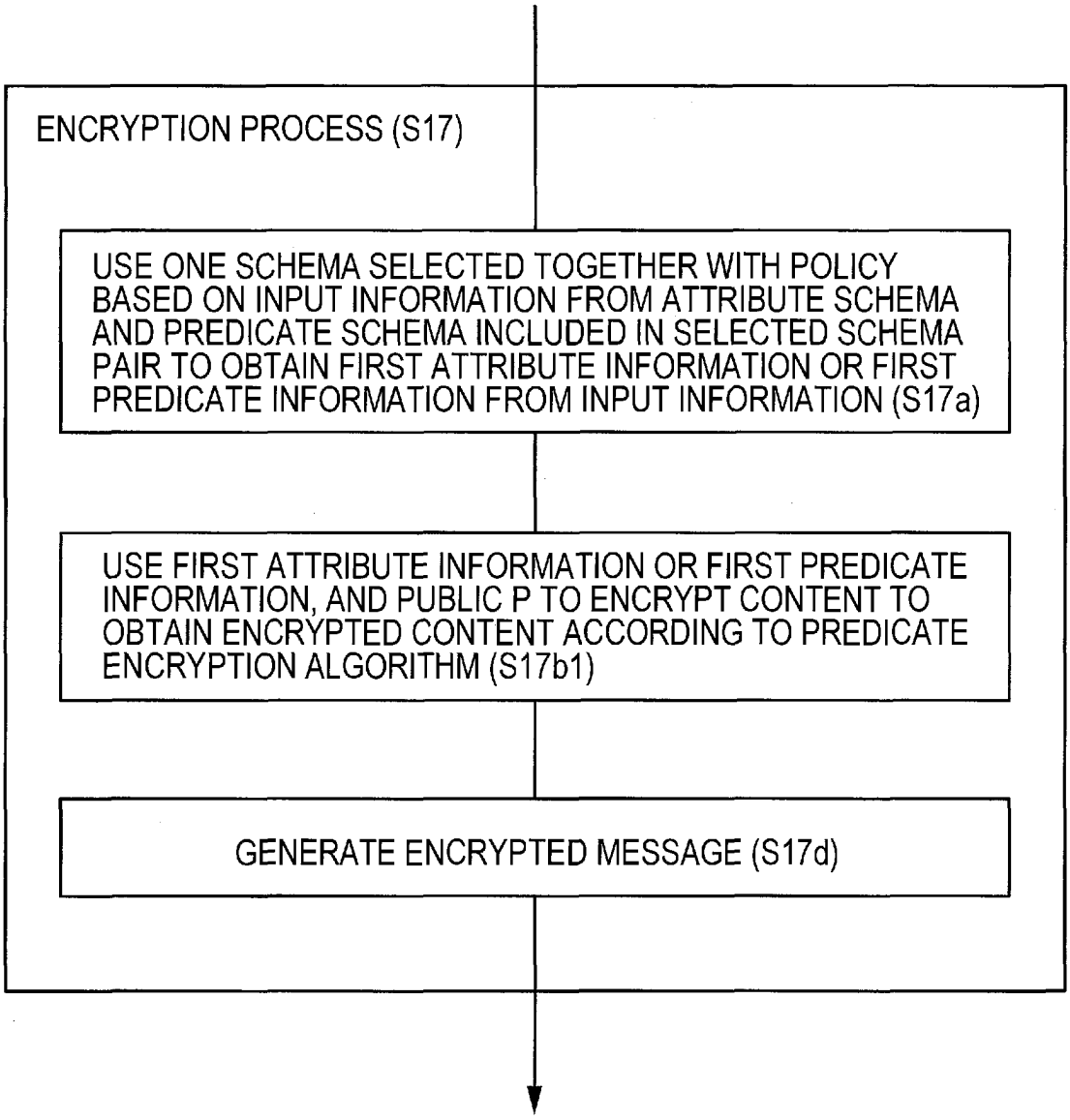

ENCRYPTION PROCESS (S17)
USE ONE SCHEMA SELECTED TOGETHER WITH POLICY BASED ON INPUT INFORMATION FROM ATTRIBUTE SCHEMA AND PREDICATE SCHEMA INCLUDED IN SELECTED SCHEMA PAIR TO OBTAIN FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION FROM INPUT INFORMATION (S17a)
USE FIRST ATTRIBUTE INFORMATION OR FIRST PREDICATE INFORMATION, AND PUBLIC P TO ENCRYPT CONTENT TO OBTAIN ENCRYPTED CONTENT ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S17b1)
GENERATE ENCRYPTED MESSAGE (S17d)

FIG.78

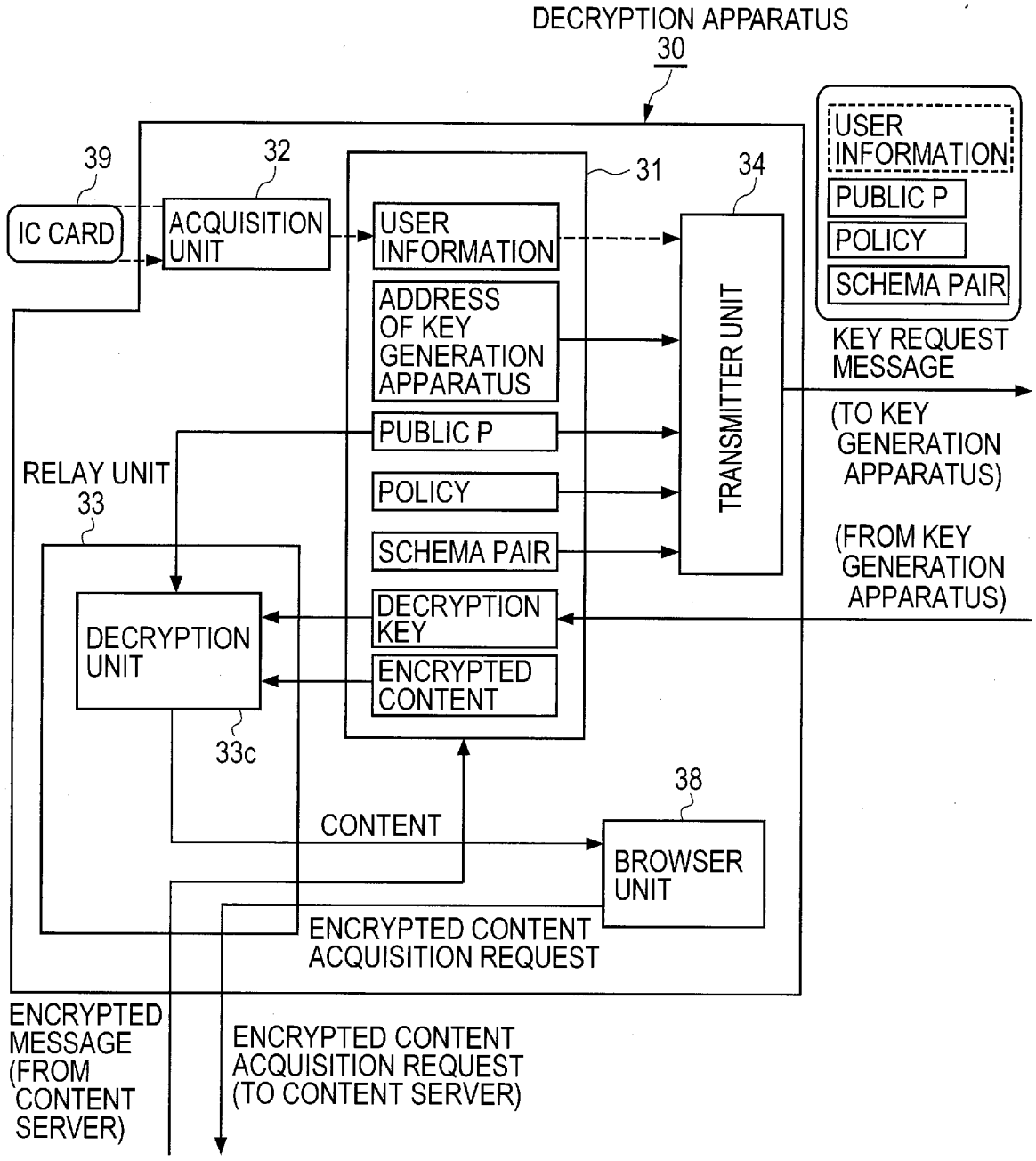

DECRYPTION APPARATUS
30
39
IC CARD
32
ACQUISITION UNIT
31
USER INFORMATION
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
34
TRANSMITTER UNIT
USER INFORMATION
PUBLIC P
POLICY
SCHEMA PAIR
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
(FROM KEY GENERATION APPARATUS)
RELAY UNIT
33
DECRYPTION UNIT
33c
DECRYPTION KEY
ENCRYPTED CONTENT
38
CONTENT
BROWSER UNIT
ENCRYPTED CONTENT ACQUISITION REQUEST
ENCRYPTED MESSAGE (FROM CONTENT SERVER)
ENCRYPTED CONTENT ACQUISITION REQUEST (TO CONTENT SERVER)

FIG.79

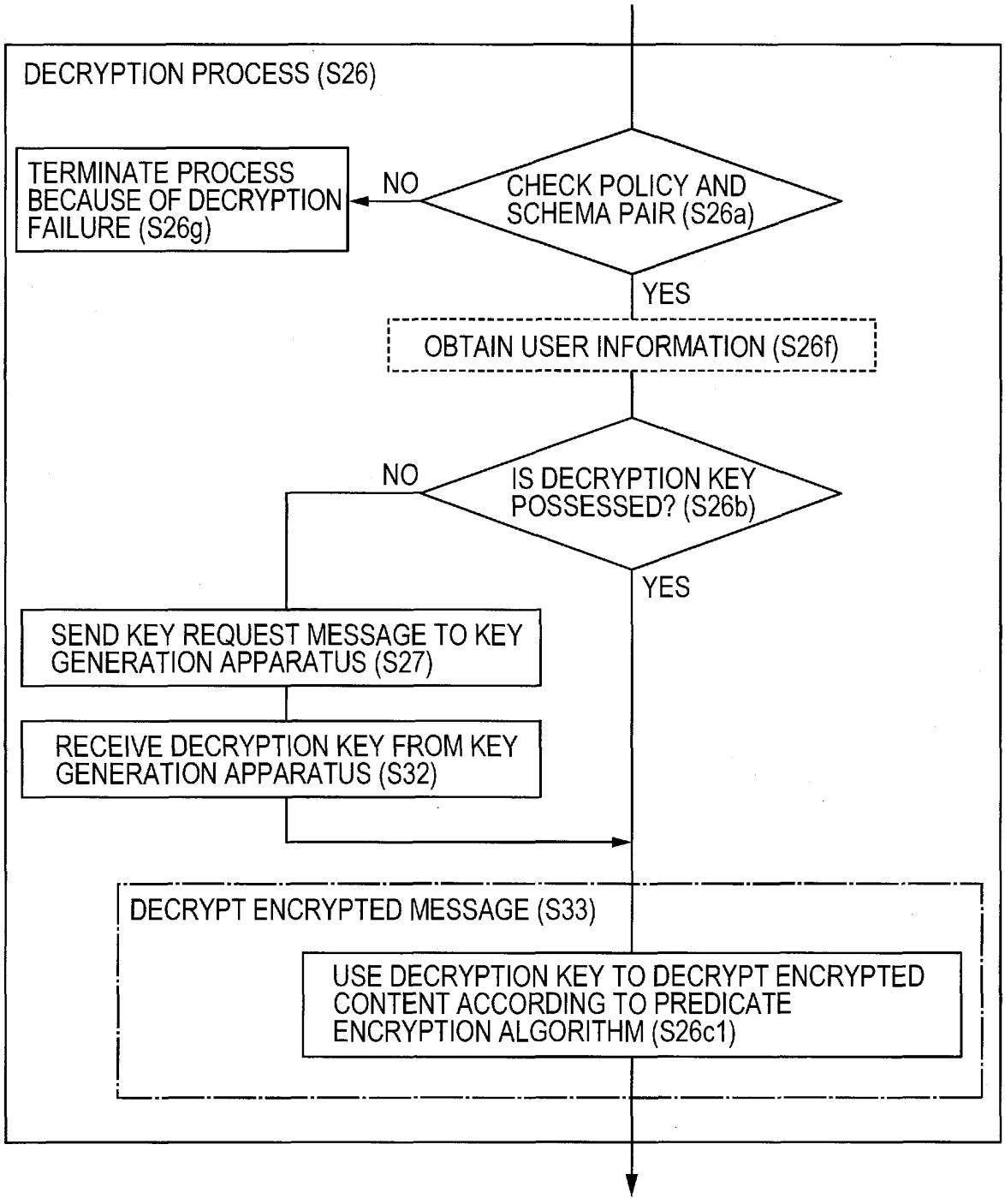

DECRYPTION PROCESS (S26)
CHECK POLICY AND SCHEMA PAIR (S26a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S26g)
YES
OBTAIN USER INFORMATION (S26f)
IS DECRYPTION KEY POSSESSED? (S26b)
NO
YES
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S27)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S32)
DECRYPT ENCRYPTED MESSAGE (S33)
USE DECRYPTION KEY TO DECRYPT ENCRYPTED CONTENT ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S26c1)

FIG.80

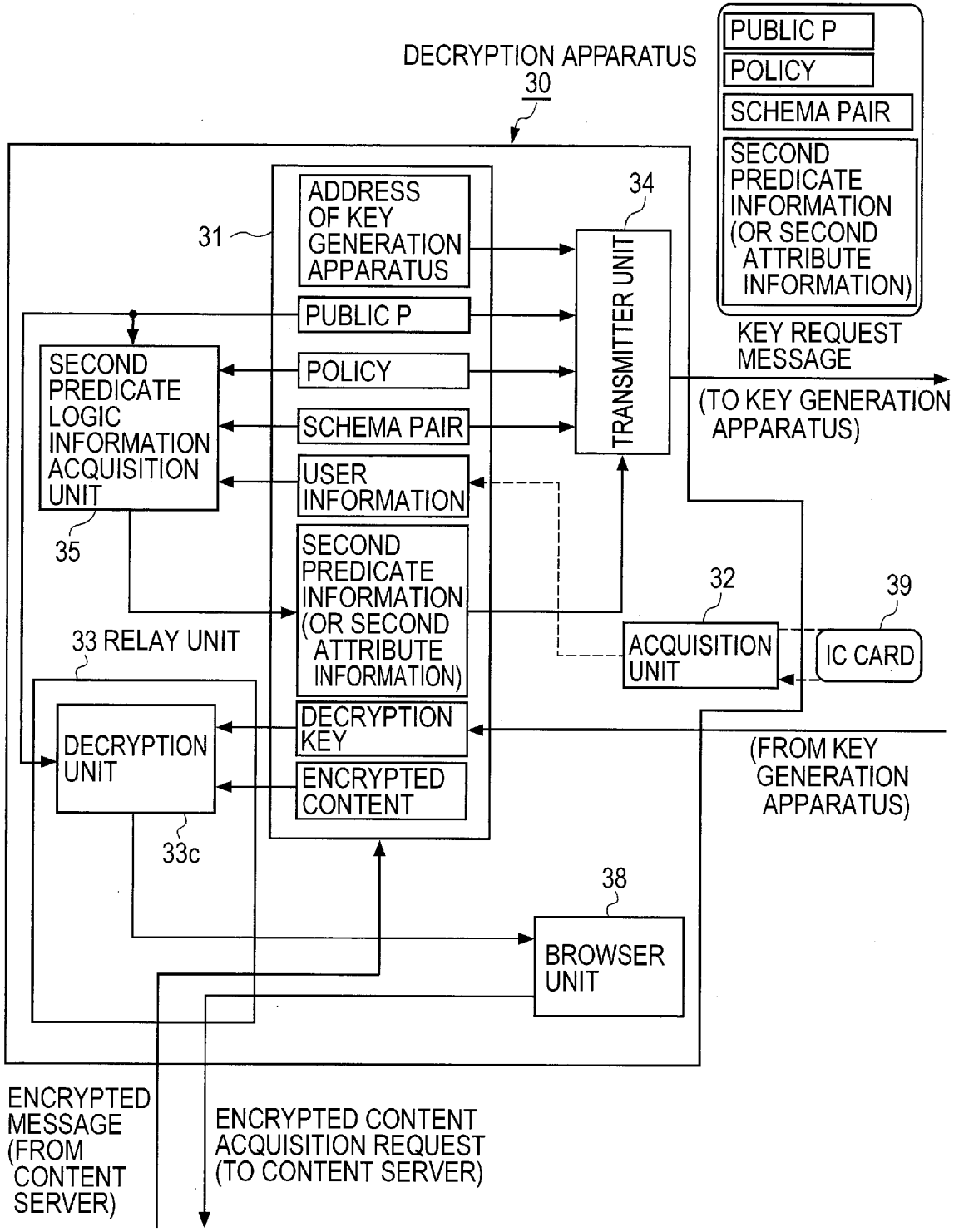

DECRYPTION APPARATUS
30
PUBLIC P
POLICY
SCHEMA PAIR
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
KEY REQUEST MESSAGE
(TO KEY GENERATION APPARATUS)
31
ADDRESS OF KEY GENERATION APPARATUS
PUBLIC P
POLICY
SCHEMA PAIR
USER INFORMATION
SECOND PREDICATE INFORMATION (OR SECOND ATTRIBUTE INFORMATION)
DECRYPTION KEY
ENCRYPTED CONTENT
34
TRANSMITTER UNIT
SECOND PREDICATE LOGIC INFORMATION ACQUISITION UNIT
35
32
ACQUISITION UNIT
39
IC CARD
(FROM KEY GENERATION APPARATUS)
33 RELAY UNIT
DECRYPTION UNIT
33c
38
BROWSER UNIT
ENCRYPTED MESSAGE (FROM CONTENT SERVER)
ENCRYPTED CONTENT ACQUISITION REQUEST (TO CONTENT SERVER)

FIG.81

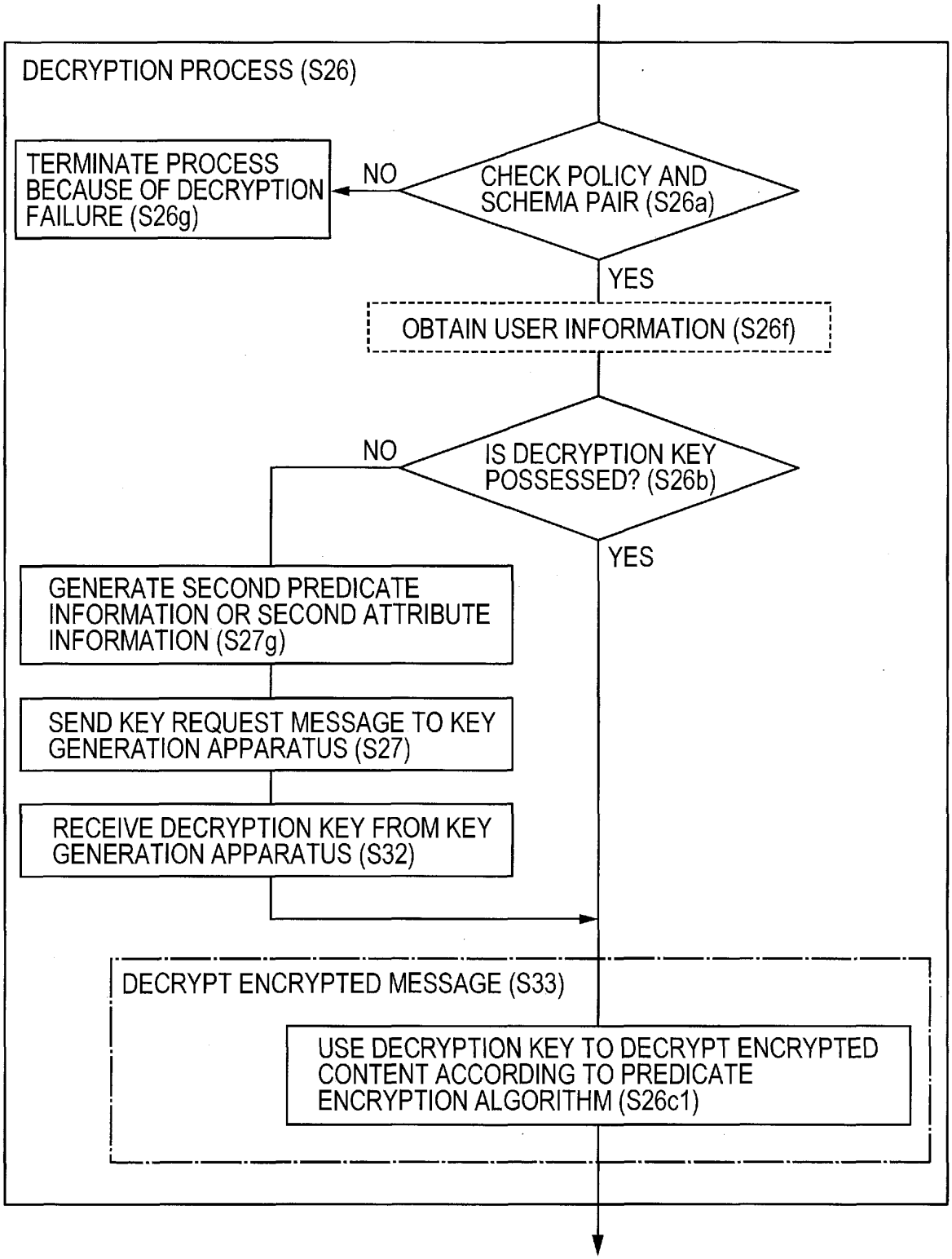

DECRYPTION PROCESS (S26)
CHECK POLICY AND SCHEMA PAIR (S26a)
NO
TERMINATE PROCESS BECAUSE OF DECRYPTION FAILURE (S26g)
YES
OBTAIN USER INFORMATION (S26f)
IS DECRYPTION KEY POSSESSED? (S26b)
NO
YES
GENERATE SECOND PREDICATE INFORMATION OR SECOND ATTRIBUTE INFORMATION (S27g)
SEND KEY REQUEST MESSAGE TO KEY GENERATION APPARATUS (S27)
RECEIVE DECRYPTION KEY FROM KEY GENERATION APPARATUS (S32)
DECRYPT ENCRYPTED MESSAGE (S33)
USE DECRYPTION KEY TO DECRYPT ENCRYPTED CONTENT ACCORDING TO PREDICATE ENCRYPTION ALGORITHM (S26c1)

FIG.82

<html>

<!–

ALGORITHM IDENTIFIER BLOCK - PREDICATE ENCRYPTION ALGORITHM FOR PRIVATE KEY - PRIVATE KEY ENCRYPTION ALGORITHM FOR CONTENT
DIGITAL SIGNATURE BLOCK
PUBLIC PARAMETER INFORMATION BLOCK
POLICY FIELD
SCHEMA FIELD
ENCRYPTION INFORMATION FIELD
CONTENT FILE NAME
CONTENT TYPE
CONTENT FILE SIZE
ATTRIBUTE FIELD
PREDICATE FIELD
ENCRYPTED CONTENT

-->

(ANY HTML SENTENCE FOLLOWS)

</html>

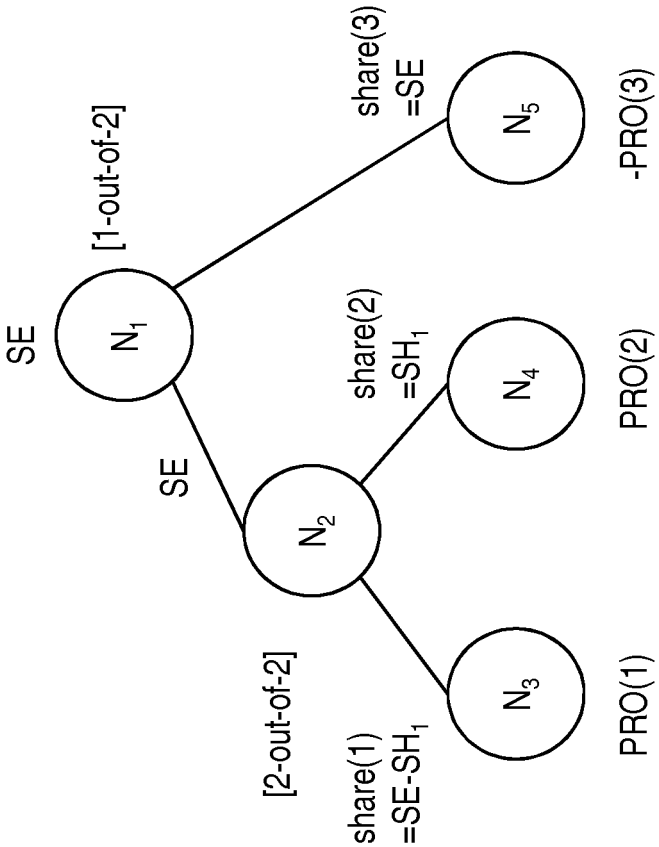

SE
N1
[1-out-of-2]
share(3)
=SE
N5
-PRO(3)
SE
N2
share(2)
=SH1
N4
PRO(2)
[2-out-of-2]
share(1)
=SE-SH1
N3
PRO(1)
PRO(1)∧PRO(2)∨¬PRO(3)

FIG. 83

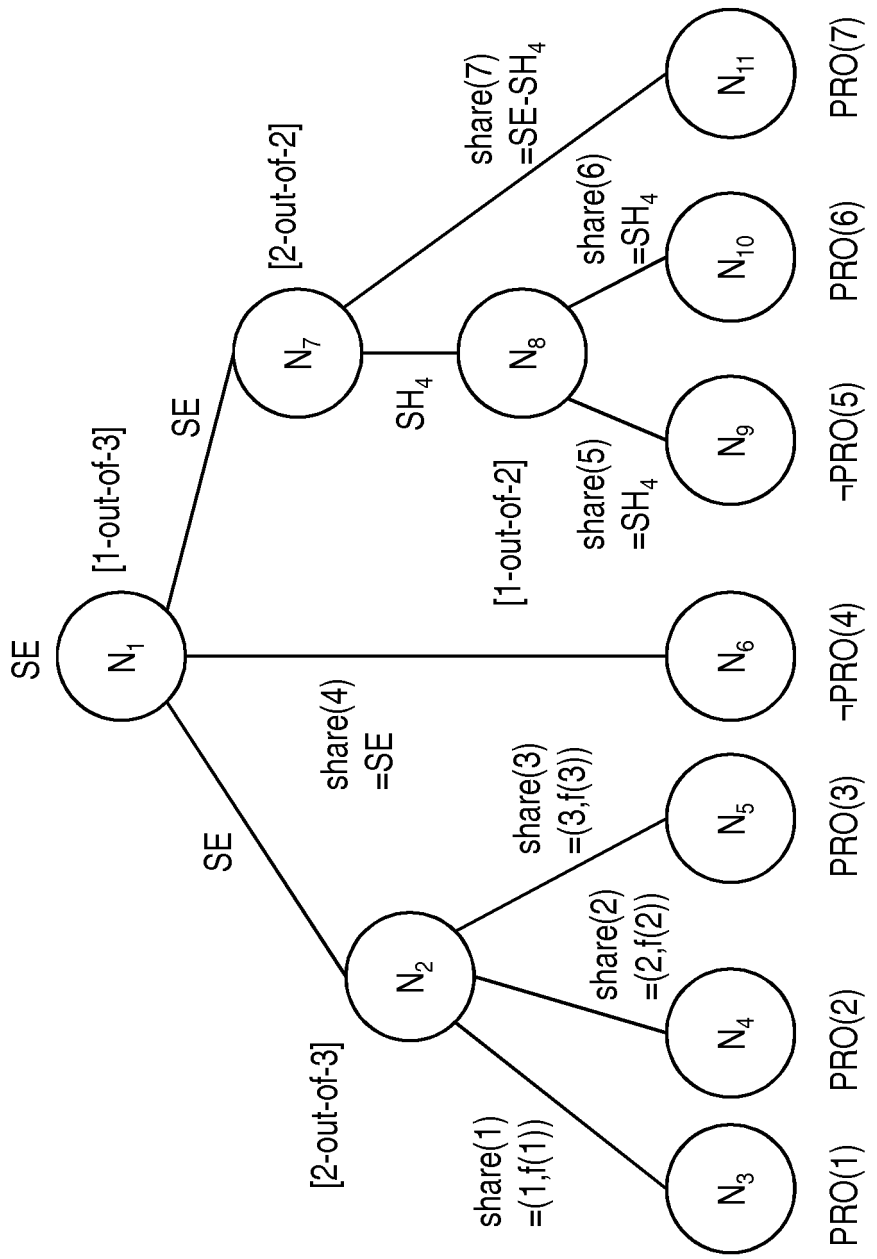

SE
N1
[1-out-of-3]
SE
SE
N7
[2-out-of-2]
SH4
N8
[1-out-of-2]
share(7)
=SE-SH4
share(6)
=SH4
share(5)
=SH4
N9
N10
N11
¬PRO(5)
PRO(6)
PRO(7)
share(4)
=SE
N6
¬PRO(4)
[2-out-of-3]
N2
share(3)
=(3,f(3))
N5
PRO(3)
share(2)
=(2,f(2))
N4
PRO(2)
share(1)
=(1,f(1))
N3
PRO(1)
PRO(1) ∧ PRO(2) ∨ PRO(2) ∧ PRO(3) ∨ PRO(3) ∨ PRO(1) ∧ PRO(3)
∨ ¬PRO(4) ∨ (¬PRO(5) ∨ PRO(6)) ∧ PRO(7)

FIG. 84

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/066716

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2011
Kokai Jitsuyo Shinan Koho 1971-2011 Toroku Jitsuyo Shinan Koho 1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII), functional encryption, attribute-based encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009/0080658 A1 (Brent Waters, et al.), 26 March 2009 (26.03.2009), all pages (Family: none)	1-39
A	Katz, J., et al., Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, Cryptology ePrint Archive, Report 2007/404, 2008.07.07, p.1-29, 4 Our Main Construction	1-39
A	Attrapadung, N., et al., Dual-Policy Attribute Based Encryption, Lecture Notes in Computer Science, Vol.5536, 2009, p.168-185, 1 Introduction, 4 Dual-Policy ABE Scheme, 6 Single-Policy Modes of DP-ABE	1-39

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 September, 2011 (13.09.11)	20 September, 2011 (20.09.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/066716

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Lewko, A., et al., Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, Cryptology ePrint Archive, Report 2010/110, 2010.03.29, p.1-56, 2 Fully Secure Attribute-Based Encryption, 3 Fully Secure Predicate Encryption	1-39
P,A	Boneh, D., et al., Functional Encryption: Definitions and Challenges, Cryptology ePrint Archive, Report 2010/543, 2011.01.04, p.1-23, all pages	1-39

Form PCT/ISA/210 (continuation of second sheet) (July 2009)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- NTT Cryptographic Primitives. Information Security Project, 15 July 2010 **[0006]**
- **J. KATZ ; A. SAHAI ; B. WATERS.** Predicate Encryption Supporting Disjunction, Polynomial Equations, and Inner Products. *Eurocrypt,* 2008, 146-162 **[0006]**
- Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption. **TATSUAKI OKAMOTO ; KATSUYUKI TAKASHIMA.** Advances in Cryptology -- CRYPTO 2010, Lecture Notes in Computer Science. Springer-Verlag, 2010, vol. 6223, 191-208 **[0032]**
- **TATSUAKI OKAMOTO ; KATSUYUKI TAKASHIMA.** Hierarchical Predicate Encryption for Inner-Products. *ASIACRYPT 2009,* 2009, 214-231 **[0035]**
- **A. SHAMIR.** How to Share a Secret. *Communications of the ACM,* November 1979, vol. 22 (11), 612-613 **[0036] [0069]**
- Efficient Non-interactive Proof Systems for Bilinear Groups. **JENS GROTH ; AMIT SAHAI.** Advances in Cryptology - EUROCRYPT. LNCS, March 2008, vol. 4965, 415-432 **[0037]**
- **ALFRED. J. MENEZES.** Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers, 61-81 **[0055] [0106]**
- **V. S. MILLER.** *Short Programs for Functions on Curves,* 1986, http://crypto.stanford.edu/miller/miller.pdf **[0055] [0106]**
- **A. MIYAJI ; M. NAKABAYASHI ; S. TAKANO.** New Explicit Conditions of Elliptic Curve Traces for FR Reduction. *IEICE Trans. Fundamentals,* May 2001, vol. E84-A (5), 1234-1243 **[0055] [0106]**
- Constructing Elliptic Curves with Prescribed Embedding Degrees. **P. S. L. M. BARRETO ; B. LYNN ; M. SCOTT.** Proc. SCN '2002. Springer-Verlag, 2003, vol. 2576, 257-267 **[0055]**
- **R. DUPONT ; A. ENGE ; F. MORAIN.** *Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields, http://eprint.iacr.org/2002/094* **[0055] [0106]**
- **KAORU KUROSAWA ; WAKAHA OGATA.** Basic Mathematics of Modern Cryptography (IEICE Lecture Series. Corona Publishing Co., Ltd, March 2004, 116-119 **[0069]**
- **IAN F. BLAKE ; GADIEL SEROUSSI ; NIGEL P. SMART.** Elliptic Curves in Cryptography. *Pearson Education,* ISBN 4-89471-431-0 **[0099]**
- Constructing Elliptic Curves with Prescribed Embedding Degrees. **P. S. L. M. BARRETO ; B. LYNN ; M. SCOTT.** Proc. SCN '2002. LNCS, 2002, vol. 2576, 257-267 **[0106]**